TAMPEREEN
AMMATTIKORKEAKOULU

TALOTEKNIIKAN KYBERTURVALLISUUS

Ari Järvinen

Opinnäytetyö
Toukokuu 2018
Talotekniikka
LVI

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Talotekniikan koulutus
Talotekniikka / LVI

JÄRVINEN, ARI:
Talotekniikan kyberturvallisuus

Opinnäytetyö 42 sivua
Toukokuu 2018

Tässä työssä tarkasteltiin talotekniikan kyberturvallisuutta. Talotekniikka on kybervaikuttamisen kannalta merkittävä riskikohde. Talotekniset järjestelmät huolehtivat muun muassa sisäilman laadusta ja vaikuttavat suoraan energiankäyttöön. Taloteknisiä toimilaitteita ohjaava rakennusautomaatiojärjestelmä sisältää paljon tietoa rakennuksen käytöstä sekä sen käyttäjien yksityisyyden suojaan kuuluvia asioita. Rakennusautomaation väärinkäyttömahdollisuuksiin ei yleensä kiinnitetä huomiota. Kaikki edellä mainitut asiat tekevät taloteknisistä järjestelmistä houkuttelevan kohteen kyberrikollisille.

Kybervaikuttamisella voidaan esimerkiksi kasvattaa energiankulutusta tai aiheuttaa materiaalista hävikkiä, mistä taloudellisesti hyötyvät rikoksen tekijät taustajoukkoineen. Manipuloimalla sisäilman olosuhteet luovia lämmitys-, jäähdytys- ja kosteudenhallintajärjestelmiä voidaan energian kulutusta kasvattaa tarpeettomasti merkittävissä määrin. Sisäilman olosuhteita ja valaistusta muokkaamalla voidaan alentaa työtehoa. Talotekniikka voi olla myös kybervaikuttamisen keinoja käyttävän valtiollisen toimijan kohteena osana hybridiuhkia.

Työn tarkoituksena oli antaa lukijoille perustietoja talotekniikkaan kohdistuvista kyberuhista sekä niihin liittyvistä riskeistä ja hallinnan mahdollisuuksista. Työssä perehdyttiin aiheesta julkaistuun kirjallisuuteen ja haastateltiin kyberturvallisuuden ja talotekniikan asiantuntijoita teoriatietojen täydentämiseksi.

Talotekniikan digitalisaatiolla saavutettavat edut ovat niin merkittävät, että sen kehittymistä ja laajentumista ei kannata estää, mutta siihen liittyvät riskit on tiedostettava nykyistä paremmin. Kyberuhkien hallitsemiseksi on käytettävissä monia mahdollisuuksia, joista tärkein on huolellinen järjestelmäanalyysi suunnitteluvaiheessa ja siinä kyber- ja tietoturvallisuuteen vaikuttavien tekijöiden huomioiminen. Teknisesti uhkia voidaan hallita taloudellisesti, mutta etenkin suuremmissa järjestelmissä inhimillinen tekijä muodostaa vaikeasti hallittavan riskin. Varalle asennettavat omavoimaiset säätimet sekä pumpuille ja puhaltimille asennetut kiinteät varasyötöt ovat hyviä varautumiskeinoja, olipa varautumiskohteena rakennusautomaation vakava häiriö, vikaantuminen tai kybervaikuttaminen. Kaikkia poikkeus- ja häiriötilanteita varten tulee laatia asianmukaiset toiminta- ja dokumentaatio-ohjeistukset, joiden käyttöä tulee myös harjoitella.

Asiasanat: talotekniikka, rakennusautomaatio, kyberturvallisuus, hybridiuhka

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Building Services Engineering
HVAC Building Services Engineering

JÄRVINEN, ARI:
The Cyber Safety in the Building Services Engineering Systems

Bachelor's thesis 42 pages
May 2018

This thesis examined the cybersecurity in the building services engineering systems (BSES). BSES presents a significant risk of cyber influencing. BSES maintains indoor air quality and has a direct effect on energy consumption.

BSES contains a lot of information about the usage of the building, including information pertaining to the privacy protection of its users. The potential abuse of this information is often overlooked. All of the aforementioned makes BSES an attractive target for cyber criminals.

Cyber influencing can be used to increase energy consumption, or cause material wastage, creating financial benefits to the criminals and their associates. Energy consumption can be significantly increased by manipulating the systems controlling indoor air heating, cooling and humidity. Working efficiency can be affected by manipulating the indoor air quality and lighting conditions. BSES can also be a target for a governmental operator using cyber influencing as part of hybrid threats.

The purpose of this thesis was to provide its readers with basic information on cyber-threats related to building services engineering systems, and the related risks and the potential of managing them. Publications relating to the subject have been reviewed and experts on cyber security and BSES have been interviewed to complete the theoretical base.

The benefits achievable with the digitalization of BSES are so significant that the digital development and expansion should not be obstructed, but people should be more aware of the associated risks. There are many opportunities available for managing cyber threats, the most important being a careful systems analysis and the observation of cyber and information security during the planning stages. Technical threats can be managed economically, but especially in larger systems the human factor creates a risk that is difficult to manage. Redundant systems with self-powered controls and backup power supplies for pumps and fans are good preparatory methods, be it for a serious malfunction, failure or cyber influencing of BSES. Proper operating and documenting instructions need to be created for all anomaly and failure situations, and the situations also need to be practiced on.

Key words: building services engineering, building automation and control systems, cyber security, hybrid threats

SISÄLLYS

1 JOHDANTO 10
2 KYBERTURVALLISUUS 12
2.1 Kyberturvallisuuteen liittyviä suunnitelmia, määräyksiä ja ohjeita sekä tutkimuksia 13
2.1.1 EU-säännökset NIS ja GDPR 13
2.1.2 Suomen kyberturvallisuusstrategia, lait ja standardit 14
2.1.3 VAHTI -ohjeistus 14
2.1.4 KATAKRI 15
2.1.5 Huoltovarmuuskeskus sekä muut laitokset ja virastot 15
2.1.6 ST-julkaisut 15
2.1.7 Valmistajien ja maahantuojien ohjeistus 15
2.1.8 Tutkimusjulkaisuja 16
3 TALOTEKNIIKAN KYBERTURVALLISUUS 17
3.1 Kenttälaitteet 20
3.1.1 Lämmitysjärjestelmä 21
3.1.2 Vesijohtojärjestelmä 22
3.1.3 Jätevesijärjestelmä 23
3.1.4 Ilmanvaihto ja ilmastointi 24
3.1.5 Jäähdytys 25
3.1.6 Sähköjärjestelmä 26
3.1.7 LED-valaistus 28
3.2 Alakeskukset sekä huone- ja yksikkösäätimet 29
3.2.1 DoS 31
3.2.2 Logiikkapommi 31
3.2.3 Väylät ja protokollat 32
3.3 Valvomot 33
3.4 Muu taloautomaatio 34
4 SUOJAUS JA YKSITYISYYS SEKÄ SOPIMUKSET 37
4.1 Fyysinen suojaus ja käyttöoikeuksien hallinta 37
4.2 Yksityisyyden suojaus 38
4.3 Sopiminen 38
5 POHDINTA 40
LÄHTEET 41

LYHENTEET JA KÄSITTEET

AI	Analoginen tulo, I/O-pisteen tyyppi rakennusautomaatiossa.
Alakeskus	Laitteisto, johon rakennusautomaatiojärjestelmän kenttäpisteet liittyvät ja jossa tietoa käsitellään ja/tai muokataan.
Algoritmi	Joukko hyvin määriteltyjä sääntöjä, joilla ongelman ratkaisu löytyy äärellisellä askelmäärällä (matemaattinen yhtälö tai yhtälöryhmä).
Analoginen anturi	Anturin toiminta ja lähtöviesti ovat analogisia.
Anturi	Laite, joka havaitsee mitattavassa tulosuureessa tapahtuvan kemiallisen tai fysikaalisen muutoksen ja muuttaa tiedon tietyn lainalaisuuden mukaiseksi lähtösuureeksi.
AO	Analoginen lähtö, I/O-pisteen tyyppi rakennusautomaatiossa.
Asetusarvo	Säätimeen asetettu, prosessin haluttua tilaa vastaava viesti tai osoitustavoitearvo.
BACnet	Building Automation and Control Networks. BACnet on 1987 kehitetty rakennusautomaation (ylätason) ja säätöpiirien tarpeisiin oleva tiedonsiirtoprotokolla, joka on ANSI-, ISO-16484-5 ja ASHRAE standardoitu
CHP	Combined Heat and Power, sähkön ja lämmön yhteistuotanto, voimalaitostyyppi.
CIA	Confidentiality, Integrity and Availability, tietoturvallisuuden pääperiaatteet ovat luottamuksellisuus, eheys ja saatavuus.
CO_2	Hiilidioksidi.
CPU-osa	Suoritin tai prosessori (engl. Central Processing Unit eli CPU) on tietokoneen osa, joka suorittaa tietokoneohjelman sisältämiä konekielisiä käskyjä.
DALI	Digital Addressable Lighting Interface. Itsenäinen, osoitteellinen valaistusohjausprotokolla, standardit IEC 60929 ja IEC 62386.
debug	Virheen jäljitys.
DI	Digitaalinen tulo, I/O-pisteen tyyppi rakennusautomaatiossa.
DO	Digitaalinen lähtö, I/O-pisteen tyyppi rakennusautomaatiossa.

Eheys	Tarkoittaa sitä, että vastaanottajalle saapuva viesti on oikea, muuttumaton.
EnOcean	Erittäin vähän energiaa kuluttava langaton tiedonsiirtotekniikka kytkimille ja antureille, joka kerää käyttöenergiansa ympäristöstä.
Ethernet	Yleisimmin käytetty pakettipohjainen lähiverkkoratkaisu (LAN).
EU	Euroopan unioni
FW	Firmware, laiteohjelmisto.
GDPR	Euroopan unionin tietosuoja-asetus (General data protection regulation).
Huonesäädin	Yhden huoneen yhden tai useamman olosuhdetekijän säädin.
Hälytys	Toiminta, joka kiinnittää huomion havaittuun epänormaaliin tilaan kuuluvalla tai näyttävällä signaalilla, mutta joka ei puutu korjaavaan toimintaan.
I/O piste	Input/Output. Rakennusautomaatiossa laitteiden ohjaukseen käytetty fyysinen kytkentäpiste, tulo- tai lähtöliityntä.
ICT	Information and communication technology, tieto- ja viestintätekniikka.
Invertteri	Vaihtosuuntaaja, muuntaa tasavirran (DC) vaihtovirraksi (AC).
IoT	Internet of Things eli esineiden Internet, käsitteellä tarkoitetaan Internet-verkon laajentumista kaikkiin laitteisiin ja koneisiin.
IP	Internet Protocol, tietoverkkoprotokolla.
KNX	Konnex, Saksassa kehitetty väyläteknologia, tarkoittaa liitettävyyttä, kytkettävyyttä ja yhteensopivuutta ja joka perustuu Batibus-, EHS- ja EIB-standardeihin. KNX on avoin standardi kotien ja kiinteistöjen rakennusautomaation ohjaukseen.
Konfiguraatio	Konfiguraatiolla tarkoitetaan laitteiston kokoonpanoa tai ohjelman asetusarvoja.
Kontaktori	Sähköisesti ohjattu sähkömekaaninen kytkin. Kuten rele, mutta suunniteltu suuremmille virroille ja jännitteille.

Konvektori	Lämpöpatteri, joka lämmittää sen kautta kiertävää ilmaa.
Käyttöjärjestelmä	Perusohjelmisto, joka mahdollistaa tietokoneen keskussuorittimen, muistien, käyttöpäätteiden ja muiden oheislaitteiden käytön sovellusohjelmissa.
LED	Light Emitting Diode, valoa säteilevä diodi.
LonWorks	Teknologia on alun perin Echelon Corporationin valmistamien logiikoiden väylätekniikka, nykyään käytössä hajautetuissa rakennus- ja teollisuusautomaatiojärjestelmissä.
LTO	Lämmöntalteenotto.
Lähetin	Laite, joka muuntaa mitattavan suureen arvon standardiviestiksi ja joka toimiakseen vaatii apuenergiaa.
M-bus	Mittaustiedon siirtoon ja etäluentaan tarkoitettu automaatioväylä.
Mittaustieto	Saadaan reaaliaikaista tietoa mm. prosessin ja tilojen lämpötiloista, paineista, pitoisuuksista, virtaamista, nesteen korkeudesta ja tilojen kosteudesta.
Modbus	Rekisteripohjainen tiedonsiirtoprotokolla, jonka avulla voidaan yhdistää verkkolaitteita keskenään.
NIS-direktiivi	Euroopan unionin verkko- ja tietoturvadirektiivi (The Directive on security of network and information systems).
Ohjaus	Ohjataan prosesseja haluttujen tavoitteiden saamiseksi, yleensä automaattisesti saadun mittaustiedon perusteella tai valvontajärjestelmän kautta asetusarvoja muuttamalla.
Ohjelma	Tietokoneelle annettu käskysarja määrättyjen toimintojen ja tehtävien suorittamiseksi.
Ohjelmallinen	Fyysisestä tiedosta johdettu tieto, kuten pistekäyntiaikamittaus, ristiriitahälytys jne.
Ohjelmisto	Suorittavia toimintoja vastaavat käskyt ja ohjelmat.
OPC	Open connectivity via open standards. Avoin väylästandardi, jota käytetään pääasiassa teollisuudessa.
Palomuuri	Palomuurin tehtävänä on rajoittaa tietoliikenne ainoastaan sallituille yhteyksille ja sallituin protokollin sekä sisällöin oman verkon osien tai ulkoisten verkkojen välillä.

Pressostaatti	Painekytkin.
Protokolla	Käytäntö tai standardi, joka määrittelee tai mahdollistaa laitteiden tai ohjelmien väliset yhteydet, ts. yhteyskäytäntö.
Regeneratiivinen	Regeneratiivisessa lämmönsiirtimessä lämpö siirtyy ainevirrasta toiseen väliaineen kautta. Pyörivä LTO-kenno iv-koneessa on yleisin sovellus.
Reititin	(Router) välittää lähiverkkojen välistä liikennettä OSI-mallin kerroksella 3.
Rekuperatiivinen	Rekuperatiivisessa lämmönsiirtimessä lämpö siirtyy ainevirrasta toiseen kiinteän väliaineen läpi. Levylämmönvaihdin kaukolämmön alajakokeskuksessa ja ristivirtakenno iv-koneessa ovat yleisimmät sovellukset.
RTU	Remote Terminal Unit. Kompakti binaarinen datan esitysmuoto.
Solmupiste/ Kenttälaite	Solmupiste koostuu mekaanisista, ohjelmallisista ja elektroniikka-osista. Laite/tunnistin/painike/ilmaisin ovat solmupisteitä.
SUPO	Suojelupoliisi.
Talotekniikka	Yhteisnimitys seuraaville järjestelmille: LVI-järjestelmät, sähköjärjestelmät sekä sähkötekniset tietojärjestelmät.
TCP	Transmission Control Protocol, tietoa pilkkova, kuljetuksesta huolehtiva ja tiedon perillä kokoava protokolla.
TCP/IP	Transmission Control Protocol/ Internet Protocol. Kahden tietoverkkoprotokollan yhdistelmä
Tietojärjestelmä	Rakennuksen sähköteknisiin järjestelmiin kuuluva osa, joka käsittää rakennusautomaatio-, tele- ja turvallisuusjärjestelmät.
Toimielin	Se osa toimiyksiköstä, joka vaikuttaa toimisuureeseen, esim. venttiili.
Toimilaite	Se osa toimiyksiköstä, joka vaikuttaa toimielimeen, esim. sylinteri tai kela.

Topologia	1) Laitteet toisiinsa liittävän kaapeloinnin fyysinen muoto (väylä, rengas, tähti, vapaa jne.) 2) Looginen topologia, protokollan määritelmä viestien liikennöintijärjestys.
UPS	Uninterruptible Power Supply, keskeytymätön tehon syöttö.
USB	Universal Serial Bus, yleinen tietokoneissa ja oheislaitteissa käytetty sarjaväylä, jonka versioiden tiedonsiirtonopeudet ja liitännät ovat erilaiset.
VAHTI	Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä, julkisen hallinnon tietoturvallisuuden ja tietosuojan kehittämisestä sekä ohjauksesta vastaavien hallinnon organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelin.
Web service	WWW-sovelluspalvelu.
Virtualisointi	Tekniikka, joka eriyttää elektroniikan, käyttöjärjestelmät ja sovellukset omiin kerroksiinsa.
VOC	Volatile organic compound, haihtuvat orgaaniset yhdisteet, yleensä haitallisina pidettyjä ilman yhdisteitä.
Väylä	Bus. Digitaalisen tiedonsiirron reitti, joka yhdistää automaatiojärjestelmän osat toisiinsa. Esimerkiksi kierretty parikaapeli tai Ethernet-lähiverkko.
YAMK	Ylempi ammattikorkeakoulu(tutkinto).
Yksikkösäädin	Yhtä prosessia säätävä laite.

1 JOHDANTO

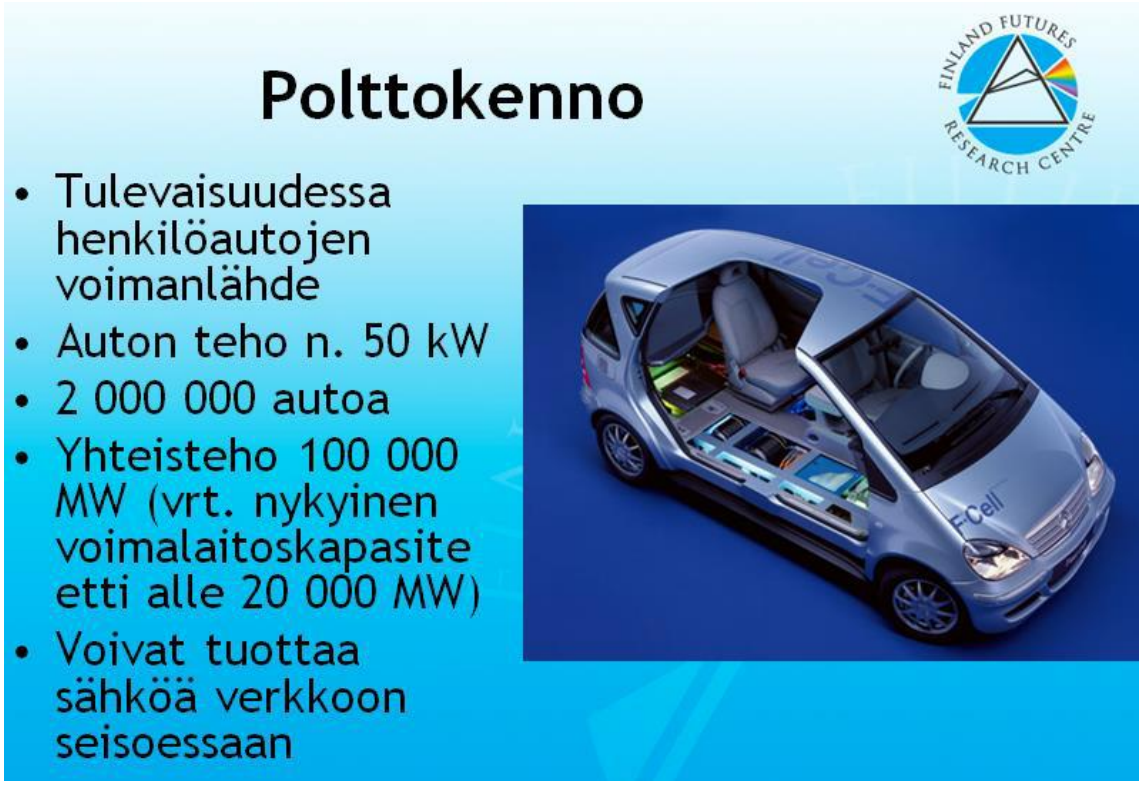
Nykypäivänä talotekniikan ohjaus on digitalisoitunutta ja automaatiotaso on usein verkottunut sekä kenttätason, että hallintotason laitteiden ja palveluiden kanssa. Digitaalisen integraation edut ovat kiistattomia, sillä sen avulla taloteknisistä järjestelmistä saa parhaan kustannushyödyn niin rakennusvaiheessa kuin etenkin käytön aikana. (ST-käsikirja 21, 9) Digitalisaatioon liittyy myös riskejä, jotka on otettava huomioon järjestelmää suunniteltaessa sekä käytettäessä, jotta esim. Lappeenrannassa taannoin tapahtuneen kerrostalon rakennusautomaatioon kohdistuneen verkkohyökkäyksen kaltaisilta seuraamuksilta voisi välttyä.

Talotekniikka on kybervaikuttamisen kannalta merkittävä riskikohde. Vaikka kyberrikollinen ei voi kuin harvoin saavuttaa välitöntä hyötyä toimillaan talotekniikkaan liittyen, ovat välillisesti saavutettavissa olevat hyödyt huomattavia. Talotekniikka voi olla myös kybervaikuttamiseen kykenevän valtiollisen toimijan kohteena osana hybridiuhkia. (ST-ohjeisto 22, 10)

Tässä työssä tarkastellaan yhtä talotekniikkaan liittyvää riskialuetta, kyberturvallisuutta, sekä kuvataan talotekniikkaan kohdistuvia kyberriskejä ja talotekniikkasuunnittelijan mahdollisuuksia niiden hallintaan. Työn tarkoituksena on kiinnittää talotekniikan suunnittelijoiksi kouluttautuvien ja muiden alalla toimivien huomiota kyberturvallisuuteen. Työn tavoitteena on antaa lukijalle perustietoja talotekniikan kyberturvallisuudesta sekä siihen liittyvästä ohjeistuksesta sekä saada heidät pohtimaan omaa suhtautumistaan talotekniikan kyberturvallisuuteen ja miettimään, miten tilannetta voi parantaa.

Työstä on rajattu pois iso osa taloautomaatiota, esim. asuntojen ja työpaikkojen LED-valaistuksen ohjaus ja säätö sekä mm. tulevaisuuden paikalliset CHP-järjestelmät. Käytettäessä uusinta LED-teknologiaa sisältyy niihin niin paljon erilaisia kybervaikuttamisen mahdollisuuksia, että aihe on useammankin opinnäytetyön laajuinen. Tässä yhteydessä LED-valaistuksen kautta vaikuttamisesta esitetään vain yksi, pieni esimerkki. Toisesta rajauksesta, eli paikallisesta CHP -tuotannosta, joka voi olla esim. polttokennolla varustetun ajoneuvon integrointi osaksi rakennuksen energiatuotantoa (kuva 1), voi todeta, että

se vaatii vastaavaa kyberriskien hallintaa kuin sähköistettyjen ajoneuvojen energiavarastojen hallinta vaatii. Muuta rakennusautomaatiota, esim. lukitusjärjestelmiä, ei käsitellä kuin kevyesti osana muuta kokonaisuutta.



KUVA 1. Polttokennollinen auto paikallisena sähköntuottajana (Kumpulainen n.d.)

2 KYBERTURVALLISUUS

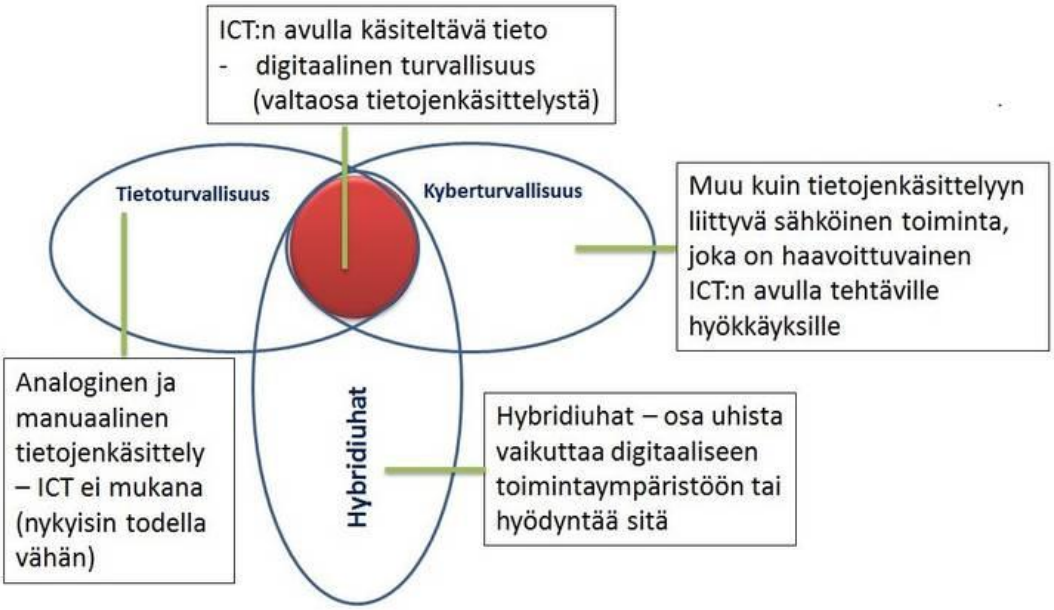
> Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristöön (sähköisessä muodossa olevan informaation (tiedon) käsittelyyn tarkoitettu, yhdestä tai useammasta tietojärjestelmästä muodostuva toimintaympäristö) voidaan luottaa ja jossa sen toiminta turvataan (Suomen kyberturvallisuusstrategia 2013, 1).

Kyberrikollinen pyrkii hyötymään taloudellisesti tavalla tai toisella niistä vaikutus- tai tiedonhankintamahdollisuuksista, joihin heille digitalisaation laajentuessa avautuu mahdollisuus. Hybridiuhissa on kyse hieman erilaisista vaikuttamisen motiiveista ja tavoitteista, mutta perimmältään siinäkin on kyse taloudellisen hyödyn tavoittelusta. Hybridiuhka voi olla kybervaikuttamisen lisäksi tai sijasta paljon muutakin vaikuttamista.

Hybridiuhkaa ei terminä ole määritelty vakiintuneella tavalla ja myös kyberturvallisuuden määritelmässä on vaihtelevuutta. Ehkä parhaiten hybridiuhan on määritellyt VAHTI-pääsihteeri Kimmo Rousku eräässä blogissaan:

> Hybridiuhissa on kyse paljon sellaisista keinoista, jotka eivät liity enää millään lailla ict- tai muuhun teknologiaympäristöön. Hybridiuhkien avulla on tarkoitus horjuttaa kohteen turvallisuustilannetta osin keinoja kaihtamatta siten, että samalla omat jäljet pyritään piilottamaan ja tällä tavalla vältetään poliittiset konfliktit, jos niin halutaan.
>
> Hybridiuhissa on kyse sellaisesta toiminnasta, jossa ei-valtiollinen tai valtiollinen toimija käyttää (harvemmin) sotilaallisia ja erityisesti ei-sotilaallisia keinoja pyrkien vaikuttamaan kohteena olevan valtion tai organisaation heikkouksiin, tavoitteena on saavuttaa toimijan asettamat omat tavoitteet. Yksi tällainen keskeinen keino > uhka on informaatiovaikuttaminen. (Rousku: Turvasatama 2017)

Tietoturvallisuuden, kyberturvallisuuden ja hybridiuhkien keskinäistä suhdetta selventää kuvio 1.



KUVIO 1. Tieto- ja kyberturvallisuuden sekä hybridiuhkien suhde. (Rousku: Turvasatama 2017)

2.1 Kyberturvallisuuteen liittyviä suunnitelmia, määräyksiä ja ohjeita sekä tutkimuksia

Kyberturvallisuuteen liittyen on laadittu määräyksiä, ohjeita ja suunnitelmia mm. EU direktiiveinä ja Valtioneuvoston periaatepäätöksenä. Kansallisen tason ohjeistusta on laatinut mm. Huoltovarmuuskeskus. Rakennusautomaation kyberturvallisuuteen on olemassa omat yleiset ohjeensa ST-kortistossa, joita täydentää valmistajien ja maahantuojien ohjeet. Talotekniikan kyberturvallisuuteen liittyviä tutkimuksia on julkaistu mm. YAMK- ja pro gradu- tasoisina tutkielmina. Ulkomaisia tutkimusjulkaisuja, joiden aiheena ovat IoT, Smart Building jne. on melko paljon.

2.1.1 EU-säännökset NIS ja GDPR

Euroopan unionin laajuisissa kyberturvallisuuden edistämispyrkimyksissä verkko- ja tietoturvadirektiivin, eli NIS-direktiivin (Direktiivi 2016/1148/EU), tavoitteena on parantaa tietoturvaa ja vähentää kyberuhkia, kun taas tietosuoja-asetuksen GDPR (Asetus

2016/679/EU) tarkoituksena on parantaa yksityisyydensuojaa ja yhdenmukaistaa tietosuojakäytäntöjä. Molemmilla on oma suotuisa vaikutus kyberturvallisuuteen, koska ne pakottavat sanktioiden uhalla rakentamaan ja korjaamaan järjestelmät paremmin kyberuhkia sietäviksi. Molemmat säännöstöt ovat oma laaja kokonaisuutensa, joista löytyy myös päällekkäisyyksiä ja jopa ristiriitoja, mutta ao. direktiivejä ei käsitellä tässä työssä sen tarkemmin, koska niiden merkitys talotekniikan suunnittelijalle kyberriskien hallinnassa on vähäinen. EU-tasoisia säännöstöjä kyberriskien hallinnan ja tietoturvan asiallisen tason saavuttamiseksi on useita, mutta niitä ei käsitellä tässä työssä.

2.1.2 Suomen kyberturvallisuusstrategia, lait ja standardit

Valtioneuvoston periaatepäätös Suomen kyberturvallisuusstrategiasta 24.1.2013 (Suomen kyberturvallisuusstrategia 2013) ohjaa ensisijaisesti yhteiskunnallisia toimijoita osana laajempaa kokonaisturvallisuuden strategiaa. Asiakirjaan kannattaa tutustua ja hyödyntää siitä mm. määritelmiä ja miettiä siinä esitettyjen mallien, visioiden yms. soveltamista omalla toimintatasolla. Sovellettavasta lainsäädännöstä ja standardeista tulee varmistua tapauskohtaisesti, mutta myöhemmin esitettävissä ST-julkaisuissa ne eritellään melko kattavasti.

2.1.3 VAHTI -ohjeistus

Valtiovarainministeriö on asettanut VAHTIn (julkisen hallinnon digitaalisen turvallisuuden johtoryhmä) (VAHTI n.d.) toimimaan julkisen hallinnon digitaalisen turvallisuuden kehittämisestä ja ohjauksesta vastaavien organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä. VAHTI on laatinut melko paljon ohjeistusta, jota voi käyttää sellaisenaan tai soveltaen myös muihin kyberturvallisuuttaa edistäviin tarkoituksiin.

2.1.4 KATAKRI

Kansallinen turvallisuusauditointikriteeristö (KATAKRI 2015) on laadittu yritysten ja muiden yhteisöjen turvallisuustason todentamiseksi viranomaisyhteistyötä varten. Kriteeristö on rinnasteinen VAHTI ohjeistuksen kanssa ja hyödynnettävissä myös muihin kyberturvallisuutta edistäviin tarkoituksiin.

2.1.5 Huoltovarmuuskeskus sekä muut laitokset ja virastot

Huoltovarmuuskeskus (HVK) on teettänyt tutkimuksia ja selvityksiä mm. energiahuollon ja teollisuusautomaation kyberturvallisuuteen liittyen (KYBER-TEO 2017.), ja ne ovat hyvin sovellettavissa rakennusautomaatioon. Muilta aloilta esim. Luonnonvarakeskus Luke on julkaissut 2017 maatalouden kyberturvallisuutta käsittelevän tutkimuksen (Laajalahti & Nikander 2017).

2.1.6 ST-julkaisut

Sähkötieto ry julkaisijana ja Sähköinfo Oy kustantajana tuottavat ja ylläpitävät käytännön läheistä julkaisusarjaa sähkö- ja tietoteknisten järjestelmien ammattilaisten avuksi. Julkaisuissa tietoturvaa käsittelevät osat sisältävät myös kyberturvallisuuteen liittyviä asioita ja niihin talotekniikkasuunnittelijan kannattaa perehtyä huolella. Hyödyllisimmät näistä julkaisuista ovat ST-kortti 710.02 ”RAKENNUSAUTOMAATION TIETOTURVA”, sekä ST-ohjeisto 22 ”Verkottuneen talotekniikan tietoturva” ja ST-käsikirja 22 ”KIINTEISTÖJEN VALVOMOJÄRJESTELMÄT”.

2.1.7 Valmistajien ja maahantuojien ohjeistus

Talotekniikan automaatiota valmistavilla ja myyvillä on omat kyberturvallisuuteen liittyvät ohjeensa. Pikaisen tarkastelun perusteella niitä ei ole julkisesti saatavilla johtuen todennäköisesti aiheen sensitiivisyydestä. Monien eri valmistajien tuotteiden kyberturvallisuutta kartoittaviin hakuihin vastauksena tuli vain linkki Viestintäviraston haavoittuvuuksista varoittaviin uutisiin tai mainoksiin, joissa kehutaan tuotetta tai palvelua, mutta

suunnittelijan kannalta mitään hyödyllistä ei ole tarjolla. Esim. eräs kotimainen automaation toimittaja kertoo käyttävänsä nykyään toisen kotimaisen valmistajan tuotetta ratkaisuna valvomon ja alakeskuksen välisen tiedonsiirron turvaamiseen, mutta ei muuta. Toinen kotimainen toimija ei taas mainitse mitään oman tuotteensa kyberturvallisuudesta, mutta vaatii sopimuksessaan, että asiakkaan on huolehdittava siitä, että heidän palveluihinsa ei voi vaikuttaa asiakasyhteyden kautta.

2.1.8 Tutkimusjulkaisuja

Edellä todettiin, että mm. Huoltovarmuuskeskus on teetättänyt tutkimuksia teollisuusautomaation tieto- ja kyberturvallisuuteen liittyen ja että ne ovat hyvin sovellettavissa talotekniikan alueella. Talotekniikan kyberturvallisuutta käsittelee mm. Janne Ollenbergin YAMK opinnäytetyö ”Verkottuneen talotekniikan tietoturva” (Metropolia 2015) ja Tuomas Tenkasen pro gradu ”Kiinteistöautomaatiojärjestelmän tietoturvakatsaus” (JYU 2016). Ollenbergin työn perusteella julkaistiin em. ST-ohjeisto 22.

3 TALOTEKNIIKAN KYBERTURVALLISUUS

Talotekniikan tarkoituksena on luoda ja ylläpitää rakennuksen, sen toimintojen ja sitä käyttävien ihmisten hyvinvoinnille tarvittavat olosuhteet sisäilman laadun (lämpötila, kosteus, haitta-aineet…) ja valaistuksen suhteen. Olosuhteet on pystyttävä ylläpitämään energiatehokkaasti ja hyvin laajasti mm. vuodenaikojen mukaan muuttuvissa ympäristön olosuhteissa. Mainitut vaatimukset voidaan täyttää käyttämällä monipuolisesti ympäristön ja sisäilmaston olosuhteita mittaavia ja niiden muutoksia ennustavia tietoja varsinaisia toimielimiä käyttävien toimilaitteiden ohjaamiseen tarvittavien algoritmien lähtötietoina rakennusautomaatiojärjestelmässä. Usein myös taloautomaatiolla sekä kotiautomaatiolla tarkoitetaan samaa, mutta rakennusautomaatio on terminä yleisempi. Tässä työssä taloautomaatiolla tarkoitetaan pelkästään LVI-järjestelmien ohjaamista laajempaa automaation kokonaisuutta, joka kattaa mm. valaistuksen ja lukitusten ohjauksen.

Taloteknisen järjestelmäkokonaisuuden toiminnan analysointia ja optimointia varten on siihen vaikuttaneet mittaustiedot ja säädön lopputulokset tallennettava usein pitkiksi ajoiksi. Talotekniset järjestelmät vaikuttavat suoraan mm. energiankäyttöön ja sen automaatio-osat sisältävät paljon tietoa rakennuksen käytöstä ja käyttäjien yksityisyyden suojan piiriin kuuluvia asioita. (ST-ohjeisto 22, 11) Rakennusautomaation suojausta ei ole aina toteutettu asianmukaisesti, joten asiaton pääsy tietoihin on mahdollista. Kaikki nämä tekevät taloteknisistä järjestelmistä houkuttelevan kohteen kyberrikollisille.

Talotekniikka on kybervaikuttamisen kannalta merkittävä riskikohde. Vaikka kyberrikollinen ei voi kuin harvoin saavuttaa välitöntä hyötyä toimillaan talotekniikkaan liittyen, ovat välillisesti saavutettavissa olevat hyödyt huomattavia. Talotekniikka voi olla myös kybervaikuttamiseen kykenevän valtiollisen toimijan kohteena osana hybridiuhkia. (ST-ohjeisto 22, 10). Talotekniikan haavoittuvuutta lisää se, että kybervaikutus voidaan kohdistaa samanaikaisesti tai sopivasti ajallisesti porrastaen laajalle maantieteelliselle alueelle, jolloin normaalit kunnossapidon resurssit eivät riitä häiriöiden poistamiseen missään kohtuullisessa ajassa ilman, että sen varalle on tehty asianmukaisia varautumissuunnitelmia ja -toimia. (ST-ohjeisto 22, 20) Olemassa oleva ohjeistus asuintalojen poikkeus- ja häiriötilanteisiin on vuodelta 1996 (LVI 01-10259), joten on melko luonnollista, että siinä ei ole huomioitu kybervaikuttamiseen varautumista. Ohjeen päivittämiselle on myös

muita perusteita, mm. lämpöpumppujen myötä tekniikkaa on tullut lisää. Vastaavaa tilanne on myös liike- ja palvelurakennuksien kohdalla.

Kyberuhkien hallitsemiseksi on käytettävissä monia mahdollisuuksia, mutta tärkeimmät niistä ovat huolellinen järjestelmäanalyysi ja siinä kyber- ja tietoturvallisuuteen vaikuttavien tekijöiden huomioiminen, niin uudiskohteissa kuin jo olemassa olevista järjestelmistä. Ohjeita ja lähdemateriaalia em. tarkoituksiin on nyt melko hyvin tarjolla esim. ST-ohjeistuksessa, mutta yleisimmin käytettävissä kuntotutkimusten ja -arvioiden tilaus- ja laadintaohjeissa ei asiaan kiinnitetä oikeastaan minkäänlaista huomiota. Tilanne on suhteellisen helppo korjata nostamalla rakennusautomaatio selkeästi yhdeksi kuntotutkimuksen vakiokohteeksi ja viitata ST-kortteihin 710.02 ja 98.17 ao. osa-alueen ohjeena sekä vaatia laadittavaksi pöytäkirjat ST 98.44 ja ST 730.05. Em. pöytäkirjojen käytettävyys paranisi, jos pelkän ruksin lisäksi kirjattaisiin miten ao. kohta on toteutettu.

Teknisesti uhkia voidaan hallita taloudellisesti tiettyyn rajaan asti, mutta etenkin suuremmissa järjestelmissä inhimillinen tekijä muodostaa ulkoisten vaikuttimien torjumisessa vaikeasti hallittavan riskin. Pääsyoikeuksien hallinta, teknisen isännöitsijän valvontavastuu jne. ovat melko edullisia toteuttaa inhimillisten tekijöiden muodostamien riskien pienentämiseksi.

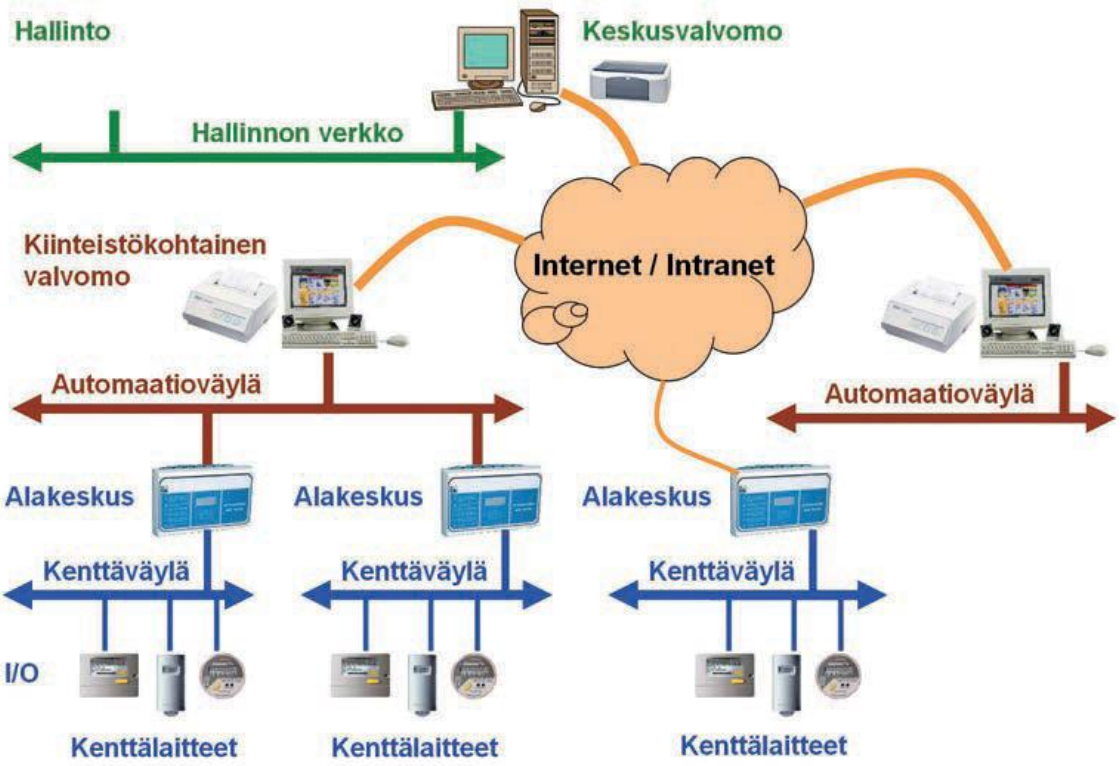
Teknisistä kyberriskeistä on paljon tietoa saatavilla suurimman osan ollessa muulla kielellä kuin suomeksi julkaistua. Inhimillisten kyberriskien hallintaan on ehkä heikoiten ohjeistusta, joka selittänee miksi enemmissä määrin kyberuhat realisoituvat hallinnollisen tietoturvan puutteiden tai laiminlyöntien seurauksena. Taulukko 1 listaa esimerkin omaisesti erilaisia väärinkäyttötapauksia ja niiltä suojaavia menetelmiä.

TAULUKKO 1. Väärinkäyttömallinnukseen pohjautuva suojautuminen (Pullinen 2012)

VÄÄRINKÄYTTÖTAPAUS	SUOJAUSMENETELMÄT
Oma työntekijä murtautuu tietoon, johon hänellä ei ole käyttöoikeuksia	Vahva tunnistautuminen, tiedostojen salaaminen, tietokantojen salaaminen, käyttöoikeuksien hallinta, käyttäjähakemiston salaaminen, lokien hallinta ja valvonta, tietokantapalvelimen ja tiedostopalvelimen kovennukset, IDS/IPS-ohjelmistojen käyttöönotto
Ulkoverkosta suoritetaan palvelunestohyökkäys verkkopalvelimeen	Www-palvelimen ja tietokantapalvelimen kovennukset, kuormantasaus, palvelin- sekä verkkolaitteistojen monistaminen, hälytysarvojen määrittäminen ja valvonta, IDS/IPS-ohjelmistot , palomuurien ja verkkolaitteiden konfiguraatiot, verkonvalvonta, www-ohjelmiston turvallinen lähdekoodi
USB-tikulta siirtyy vakoiluohjelma työasemaan, jolla tietojärjestelmää käytetään	ajantasaiset virustorjuntaohjelmistot työasemissa ja palvelimissa, USB-laitteiden hallintaohjelmisto, työaseman kovennukset, IDS/IPS-toteutukset, työasemapalomuuri, verkkolaitteiden konfiguroiminen siten, ettei vakoiluohjelma pääse lähettämään tietoa paluuliikenteenä, ajantasaiset työaseman tietoturvapäivitykset
Tietokantaan suoritetaan SQL-injektio verkkopalvelimen kautta	turvallinen ohjelmakoodi, tietokantaohjelmiston tietoturva-asetukset, verkkopalvelimen konfiguraatio, käyttöoikeuksien rajaaminen, erikoismerkkien ja epävalidien arvojen syöttämisen estäminen

Energian käyttöön liittyy useita vaikuttamisen mahdollisuuksia, mutta ne eivät yleensä kohdistu johonkin henkilöön tai hyödytä suoraan kyberrikollista, joka toiminnasta on käytännön tasolla vastuussa. Yleensä hyötyjänä on taho, jonka etujen mukaista on, että esimerkiksi joku henkilö ei kykene töihinsä haluttuna hetkenä tai että sähkönkulutusta lisätään tarpeettomasti korkean markkinahinnan aikana. (ST-ohjeisto 22, 22)

Vaikka kyberriskit ulottuvat kaikkiin verkotettuihin ja prosessointikykyä omaaviin laitteisiin, niin seuraava kyberturvallisuuden tarkastelu on pyritty tekemään rakennusautomaation hierarkian mukaisesti (kenttälaitteet, alakeskukset ja valvomot) pääjärjestelmittäin (lämmitys, käyttövesi ja viemäröinti, ilmanvaihto ja ilmastointi, jäähdytys ja sähkö). Koska älykkäät sensorit ja toimilaitteet sekä monet muut verkotettavat toiminnot eivät noudata enää perinteistä hierarkkista rakennetta (kuva 2), on käsittelyssä paljon poikkeamia. Kunkin alueen sisällä käsitellään siihen ominaisesti kuuluvia tekijöitä kuten esim. ohjelmistoja ja tiedonsiirtoa sekä talotekniikkasuunnittelijan mahdollisuuksia vähentää kyberriskien vaikuttavuutta.



KUVA 2. Rakennusautomaation hierakinen rakenne (ST-käsikirja 21, 10)

3.1 Kenttälaitteet

> Kenttälaitteiden avulla kerätään tietoa prosesseista (mittausanturit ja -lähettimet, hälytyskoskettimet, liiketunnistimet jne.) ja ohjataan niiden toimintaa (pellit ja venttiilit toimilaitteineen, kontaktorit jne.). (ST 98.17 2018, 3)

Kenttälaitteet voivat olla liityntätavaltaan joko väylälaitteita, esim. M-bus, Modbus/TCP jne., tai analogisia, esim. termistoreja. Analogisiin antureihin ei kybervaikuttaminen ulotu, jollei sitten esim. niitä syöttävää vakiovirta- tai -jännitelähdettä pääse manipuloimaan väärän mittaustuloksen aiheuttamiseksi. Sen sijaan analogisesti ohjattavat toimilaitteet voidaan asettaa väärään tilaan niitä ohjaavaan huonesäätimeen tai alakeskukseen kohdistetulla kybervaikuttamisella.

Väylään kytkettävät kenttälaitteet sisältävät aina jonkinasteisen prosessorin, joka toimii sille laaditun ohjelman mukaisesti. Jos kenttälaitteen ohjelmistossa on mihin tahansa tarkoitukseen (debug, FW-päivitys jne.) suunniteltu rajapinta, niin siihen kytkeytymällä toimintaan voi vaikuttaa. Langallisesti kytkettyjen kenttälaitteiden kohdalla tällainen riski

on melko pieni, mutta langattomien antureiden kohdalla riski on selvästi suurempi. Kytkeytymistä helpottaa huomattavasti, jos käyttäjätunnukset ja niiden salasanat ovat käyttöönoton jälkeen tehdasasetuksissa. Automaatiojärjestelmää käyttöönotettaessa on aina muistettava vaihtaa salasanat ja tallettaa ne sovitusti turvalliseen, mutta käytettävään paikkaan.

Talotekniikan käyttämät väylät eli verkot voivat itsessään tarjota arvaamattoman reitin muuten suojattuun kohteeseen, esimerkiksi vaikka ihan tavalliseen kotiin, johon näkymistä rajoitetaan verhoin tai josta keskustelujen ei haluta kuuluvan kaikille. Kannettavan tietokoneen kameran huomaa jo moni pimentää silloin, kun sitä ei käytetä, mutta miten toimia IP-verkkoon liitetyn, mahdollisesti kaksisuuntaisen ovipuhelinjärjestelmän suhteen? Vaikka tällaisen median väärinkäytön riski on pieni verrattuna esimerkiksi älytelevision avulla kerättävien katselutietojen sekä mahdollisen ääniohjauksen mikrofonin tai integroidun Skype -kameran kautta saatavien tietojen väärinkäytölle, niin mahdollisuus on ainakin otettava huomioon.

3.1.1 Lämmitysjärjestelmä

Lämmitysjärjestelmää ohjaavaan automaatioon liittyviä kenttälaitteita ovat ensisijaisesti lämpötilaa mittaavat anturit sekä venttiilejä käyttävät säätömoottorit tai moottorien ohjauskontaktorit. Muita tyyppejä ovat mm. painetta ja virtausta mittaavat anturit. Esim. vesikiertoisesta järjestelmästä energiankulutusta määritettäessä mitataan kaksi lämpötilaa (meno ja paluu) sekä tilavuusvirta, joka korjataan siirtoaineen mukaisilla kertoimilla lämpömassavirraksi. Paineen mittaus voi olla myös varotoimi, mutta lämpöpumpuissa paine on usein laitteiston toimintaa ohjaava suure. Ylilämmöltä suojaavat laitteiston osat ovat, tai ainakin pitäisi olla, automaatiosta riippumattomasti toimivia, joten niihin kybervaikuttaminen on melko hankalaa.

Säätömoottorit voivat ohjata esim. kaukolämmön ensiöpiirin venttiilejä ulkolämpötilan ja mahdollisen kompensoivan sisälämpötilan perusteella. Säätö voi olla tilaohjattua, jolloin toimilaite ajaa auki tai kiinni niin kauan, kun ohjaussuunta on aktiivinen. Säätöarvo voidaan myös asettaa jännite- tai virtaviestillä, jolloin toimilaite ajaa omassa ohjauksessaan venttiilin asetusarvoon.

Langallisesti ja analogisesti huonesäätimeen tai automaation alakeskukseen liittyvät kenttälaitteet ovat kybervaikuttamisen kohde vain niitä ohjaavaan säätimeen tai keskukseen kohdistuneen kybervaikuttamisen myötä. Väylään liitettyjen kenttälaitteiden kohdalla vaikuttamisen helppous ja siten myös todennäköisyys kasvaa, kun yksi ”suojaava” välikerros jää pois. Langattomasti muuhun automaatioon liittyvät kenttälaitteet ovat kuin väyläliityntäisiä kenttälaitteita sillä erotuksella, että niihin vaikuttamiseksi ei tarvita fyysistä yhteyttä, ts. tilasuojauksen merkitys on toisenlainen.

Kybervaikuttamisella voidaan pyrkiä esimerkiksi säätämään ostoteho tarpeettoman suureksi tai katkaisemaan lämmönjakelu. Vaikutus voidaan tehdä siten, että valvomoon siirtyy oikealta vaikuttavaa tietoa säädön tilasta, vaikka toimilaitteet ovat muussa asennossa, jolloin valvomon henkilöstö tai ohjelma ei pysty reagoimaan tilanteeseen. Toimilaitteen kesto voidaan myös asettaa koetukselle jatkuvalla värähtelynomaisella ohjauksella, mutta tätä ei voi pitää kovin todennäköisenä vaikutustapana.

Sen lisäksi, mitä automaatiojärjestelmän tieto- ja kyberturvallisuuden eteen voi tehdä, voi myös talotekniikkasuunnittelija ottaa huomioon kybervaikuttamisen riskejä. Esimerkiksi lämmitysjärjestelmän veden lämpötilaa voi säätää omavoimaisilla, termostaattisilla venttiileillä, jolloin automaatioon kohdistuva vaikutuspyrkimys on tehoton. Koska automaation edut sen toimiessa ovat kiistattomat, niin pääsääntöisesti toimilaitteet ovat automaation ohjauksessa. Niiden rinnalle asennettuna ja vain tarpeen mukaan nopeasti käyttöön otettuna omavoimaiset voivat pelastaa tilanteen, kun automaatio ei syystä tai toisesta ole käytettävissä. Sama koskee myös kiertovesipumppuja, joiden pyörimisnopeutta voi säätää taajuusmuuttajan avulla haluttua toimintapistettä tavoiteltaessa. Taajuusmuuttajaohjatun pumpun rinnalle asennettu ja vain tarpeen mukaan käyttöönotettava kiinteän pyörimisnopeuden pumppu on melko pieni lisäkustannus, mutta varmentaa merkittävästi lämmitysjärjestelmän toimintaa vika- tai häiriötilanteissa.

3.1.2 Vesijohtojärjestelmä

Vesijohtojärjestelmään pätee sama, mitä lämmitysjärjestelmään. Kiertovesipumppu (lämmin vesi) ei ole kriittinen järjestelmän toiminnan kannalta, eikä sen pyörimisnopeutta yleensä säädetä käytön aikana, mutta vesijohtoverkoston painetta voi joutua korottamaan

paineenkorotuspumpuilla. Sekä ne, että niiden toimintaa automaation kautta ohjaavat paineanturit voi varmentaa säätymättömillä pumpuilla ja pressostaateilla. Kuvassa 3 on esimerkkinä Danfoss IHPT venttiili, joka soveltuu kaukolämpöjärjestelmässä lämpimän käyttöveden omavoimaiseksi säätimeksi.

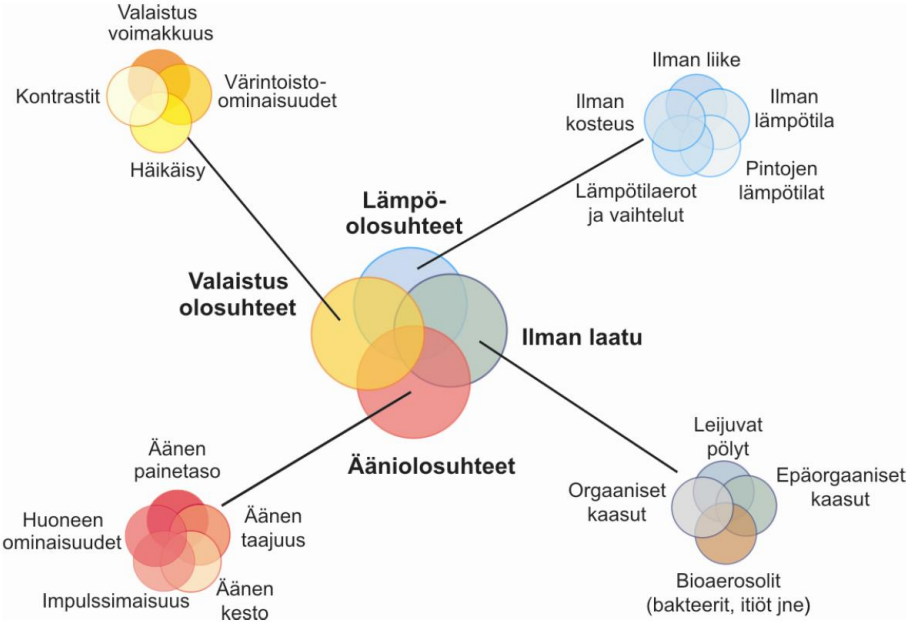
KUVA 3. Omavoimainen lämpimän käyttöveden säädin kaukolämpöjärjestelmään. (Danfoss n.d.)

3.1.3 Jätevesijärjestelmä

Jätevesijärjestelmään pätee sama, mitä vesijohtojärjestelmään paitsi viettoviemäröintiin, jossa ei ole yhtään kohtaa, johon kybervaikuttamista voisi kohdistaa. Paineviemäreissä pumppaamot ovat otollinen kohde haitan aiheuttamiseen. Pienpumppaamot ovat harvoin ulkoisen valvomon ohjauksessa, mutta tilatietoa pinnan korkeudesta ja pumpun toiminnasta valvomot kyllä saavat. Vaikka kybervaikuttamisen mahdollisuudet ovat melko vähäiset pienten jätevesipumppujen kohdalla, on ne silti syytä ottaa huomioon. Jätevesipumppaamojen toimintahäiriöt uhkaavat ja vaarantavat terveyttä vakavasti, jos etenkin isommat jätevesipumppaamot ja -viemärit tulvivat ympäristöön tai rakennukset saastuvat jätevesistä.

3.1.4 Ilmanvaihto ja ilmastointi

Ilmanvaihtoon ja ilmastointiin pätee sama, mitä lämmitysjärjestelmään. Ilmastointia voidaan säätää monipuolisen anturitiedon perusteella, joka kertoo ilmasta lämpötilan lisäksi esim. kosteuden sekä CO_2- tai VOC-pitoisuudet. Kuvassa 4 esitetään sisäilmaston tärkeimmät osa-alueet, joista ainakin osaan voidaan kohdistaa kybervaikutusta. Ilmastointia ohjaavista kenttälaitteista vain lämpötilan mittaus voidaan tehdä analogisesti ja muiden antureiden tuottama informaatio tuotetaan lähes aina välillisesti joko jonkun muunnoksen avulla, esim. kapasitanssi vs. jännite, tai prosessorien ajaman ohjelman ja jonkun sopivan ilmaisimen antaman tiedon avulla.



KUVA 4. Sisäilmaston osa-alueet (VTT ToVa-käsikirja, 2007, 29)

Ilmastoinnin toimintaa säätävät toimilaitteet voivat olla melko nopealiikkeisiä, joten niiden vaurioittaminen kybervaikuttamisen keinoin on suurempi riski kuin lämmitysjärjestelmissä. Pumppuja vastaavat puhaltimet eivät sen sijaan ole kovin arkoja ON-OFF tyyppiselle vaikuttamiselle, mutta jos sellaisen taajuus on sopiva, ylikuumenee puhaltimien moottorit liikaa, jolloin niiden sisäisen turvallisuusmekanismin toiminta ratkaisee vaurioitumisen mahdollisuudet. Liiallisen, (ulko-)ovien avaamisen estävän alipaineen voi estää puhaltimilta sähkönsyötön katkaisevalla sähkömekaanisella paine-eromittarilla myös niissä tilanteissa, joissa automatiikka toimii virheellisesti.

Ilmastointiin liittyy yleensä aina lämmön talteenotto (LTO), joka voi olla toteutettu rekuperatiivisesti, regeneratiivisesti tai epäsuorasti rekuperatiivisenä. Epäsuora rekuperatiivnen eli nestekiertoinen LTO sekä tuloilman esi- ja jälkilämmitys sekä jäähdytys nestekierrolla toteutettuna vastaavat lämmitysjärjestelmää niin riskien kuin niiden hallitsemisen kannalta. Muissa LTO-ratkaisuissa on lämpötilasuhteeseen vaikuttavia säätöpeltejä tai kennon pyöritysmoottoreita, joihin kohdistetulla kybervaikuttamisella voidaan aiheuttaa laitteiston vikaantuminen tai energiankulutuksen lisäys.

Myös tuloilman kosteuden hallintaan käytettävä kostutusjärjestelmä voi olla kybervaikuttamisen kohde. Liiallinen kostutus muokkaa työskentelyolosuhteet huonoiksi ja voi aiheuttaa huomattavia materiaalisia tappioita, kuten myös liian alhainen kosteus voi aiheuttaa turhaa hävikkiä ja sairastelua. Kosteuden hallinnan kenttälaitteet ovat hyvin otollinen kohde aiheuttaa haittaa ja vahinkoa ihmisille ja omaisuudelle kybervaikuttamisen keinoin.

3.1.5 Jäähdytys

Jäähdytykseen pätee sama, mitä lämmitysjärjestelmään ja ilmastointiin. Jäähdytys voi olla osa ilmastointia, mutta se voidaan toteuttaa myös siitä erillisenä, suorana tai välillisenä jäähdytyksenä. Kuten kosteudenhallinnalla, niin myös jäähdytyksellä tai sen puutteella voi aiheuttaa jopa sietämättömät työskentelyolosuhteet ja yhdistettynä kosteudenhallinnan manipulointiin, ovat haittavaikutukset helposti moninkertaiset. Mikäli lämmitys ja jäähdytys saadaan ohjattua toimimaan samanaikaisesti, kasvaa energiakulutus huomattavasti ilman, että käyttäjä välttämättä huomaa mitään poikkeavaa sisäilman olosuhteissa. Hyödyn kasvaneesta energiankulutuksesta saa joku muodossa tai toisessa.

Jäähdytyksessä käytettävät kompressorit vaurioituvat herkemmin katkokäytöstä kuin pitkäkestoista käynti- ja lepojaksoista, sillä käynnistyksessä voitelu on aina heikompaa kuin tasaantuneessa käynnissä. Vaikuttamalla pysäytys- ja käynnistyssykliin esim. paine- tai lämpötila-anturin tuottamaa mittaustietoa vääristämällä, voi kompressorien elinkaari lyhentyä merkittävästi.

Jäähdytyksen kylmäainepiireissä on käytettävissä omavoimaisia säätölaitteita esimerkiksi höyrystin- ja lauhdutinpaineen säätöön tai paisuntaventtiileinä (Hakala & Kaappola

2013, 116, 118, 128). Kompressorien tilavuustuottoa ei voi kaikissa tyypeissä säätää ilman automaation sähköistä ohjausta, mutta esimerkiksi ruuvikompressorien ohitusmagneettiventtiileillä voidaan tehoa säätää yhdessä tai kahdessa portaassa. Epäsuorassa jäähdytyksessä kylmävesivaraajan suurempi koko mahdollistaa sähköisen säätöjärjestelmän häiriötilanteessa kompressorien ON-OFF käytön pitempään ilman, että kuluttavia käynnistyksiä tapahtuu sallittua tiheämmin.

3.1.6 Sähköjärjestelmä

Sähköjärjestelmään liittyviä kenttälaitteita ovat esim. kontaktorit ja puolijohdekytkimet sekä tehonsäätökomponentit. Sähkömekaaniset komponentit, kuten kontaktorit, voivat vaurioitua tiheän, jopa resonanssitaajuudella tapahtuvan ohjauksen seurauksena. Puolijohdekomponentit voivat puolestaan lämmetä liikaa, jos niiden ohjaustaajuus on liian suuri tai tilan muutosnopeus on liian hidas. Suurempi vahinko voi aiheutua ohjattavan induktiivisen kuorman tuottamista jännitepiikeistä tai kapasitiivisen kuorman aiheuttamista virtapiikeistä, jotka voivat vaikuttaa laajalti piirin muihin komponentteihin.

Useimmiten kontaktorit ja muut sähköjärjestelmän kenttälaitteet on kytketty huonesäätimiin tai alakeskuksiin ilman, että ne olisivat väyläohjattuja, mutta suuntaus on väyläohjauksen yleistymiseen. Vaikka uusimpiin väyläratkaisuihin saa jo melko hyviä suojausmekanismeja väärinkäytöksien varalle, käyttöön on jo ehditty ottaa melko paljon toteutuksia, jotka altistuvat kybervaikutukselle.

Myös sähköjärjestelmään liittyville kenttälaitteille voi tehdä varajärjestelyt, jotka voivat pelastaa pahimmalta. Valojen ohjaukseen liittyen huoneeseen voi jättää esim. yhden hehkulanka- tai loisteputkilamppua käyttävän valolähteen, jota ohjataan perinteisesti katkaisimella. Myös ohituskytkennät, niin sähköiset kuin vesijohtotekniset, kannattaa ottaa huomioon suunnitelmissa ja toteutuksissa sekä sähkölämmitysten, että sähköisesti ohjattavan venttiilien kohdalla. Muuten esim. hyvää tarkoittava, sähköisesti ohjattava päävesijohdon KOTONA – POISSA venttiili voi muodostua hyvinkin houkuttelevaksi kybervaikutuksen kohteeksi tai muuten vain harmittavaksi kapistukseksi.

Mikäli kiinteistössä tuotetaan omilla järjestelmillä sähköä, esim. aurinkopaneeleilla, niin niihin liittyvät kyberriskit on otettava huomioon vastaavalla tavalla kuin minkä muunkin

automaatioverkkoon kytketyn laitteen kohdalla tehdään. Kuvassa 5 on Tivi -lehdessä 4.5.2018 julkaistu artikkeli aurinkosähköjärjestelmän haavoittuvuuksista.

tivi

TIETOTURVA Kari Kortelainen 4.5. klo 18:18

Sähköjärjestelmän tietoturva murtui minuuteissa – hakkerit voivat päästä kaatamaan koko verkon

Kaupallisten aurinkosähköjärjestelmien invertterit eivät vaikuta kovin tietoturvallisilta. Saksalaisen luokituslaitoksen TÜV Rheinlandin asiantuntijat ovat onnistuneet hakkeroimaan ne muutamassa minuutissa. Erityisen huolestuttavaksi tiedon tekee se, että yleensä invertteriin ovat viestiyhteydessä energian varastointijärjestelmät.

Vihamielinen hyökkäys voisi periaatteessa aiheuttaa monenlaista vahinkoa alkaen aurinkosähköjärjestelmän tehon manipuloinnista aina varastointijärjestelmän vahingoittamiseen, mikä voisi puolestaan pahimmillaan lamauttaa sähköverkon täysin.

"Haavoittuvuuksien kartoittaminen on välttämätöntä, kun verkossa on miljoonia uusiutuvan energian tuottajia, jotka ovat riippuvaisia älykkäästä sähköverkosta. Lisäksi käytössä on jo yli 75 000 kotien energiavarastoa", TÜV Rheinlandin testausjohtaja **Daniel Hamburg** sanoo.

"Aurinkosähkön tuottajien pitää pystyä viestimään verkon toimittajan kanssa turvallisesti ja virheettömästi, niin että energian syöttö verkkoon tapahtuu sovitulla tavalla."

Invertteri muuttaa aurinkopaneelin tuottaman tasasähkön vaihtosähköksi ja syöttää sen verkkoon. Invertterien hakkeroinnilla on mahdollista päästä kiinni myös akkujen hallintajärjestelmään. Hyökkääjä voi pakottaa akun epävakaaseen tilaan ja sitä kautta häiritä koko sähköverkkoa aiheuttamalla hallitsematonta tehon vaihtelua.

Aurinkosähköjärjestelmien komponenttien normaali toiminnallisen turvallisuuden tarkastus ei sisällä kyberturvallisuuden varmistusta.

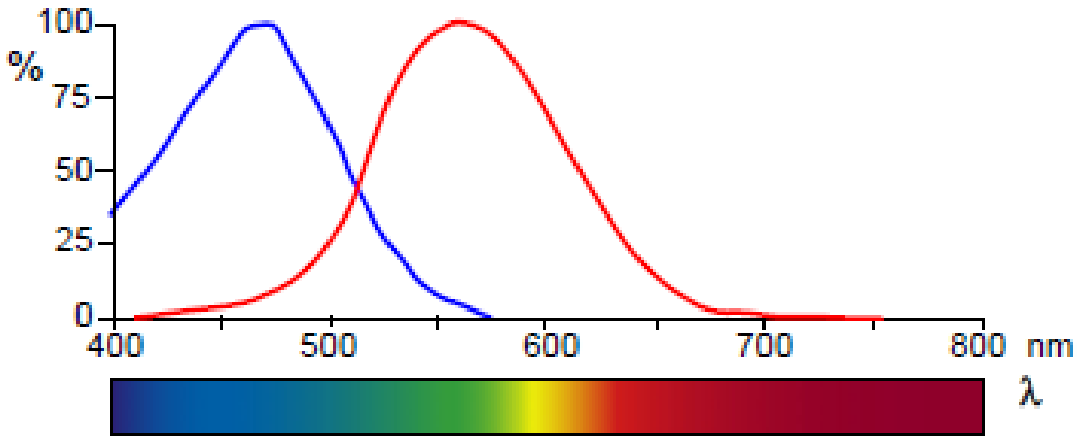
TÜV suosittelee aurinkosähköjärjestelmien valmistajille järjestelmien tarkistamista ja mahdollisten haavoittuvuuksien korjaamista.

KUVA 5. Aurinkosähköjärjestelmien invertterit ovat kyberriski

3.1.7 LED-valaistus

On yleisesti tiedossa, että valaistuksen intensiteetin nopea vaihtelu (välkkyminen) voi altistaa migreenille sekä epileptisille kohtauksille ja LEDit ovat mitä soveltuvimpia valolähteitä nopeaan ohjaukseen. Jos yleistyvän LED-valaistuksen ohjausjärjestelmää pääsee manipuloimaan, voi sitä kautta vaikuttaa esim. henkilön terveyteen ja työkykyyn.

Valon määrän ja värilämpötilan säätäminen esim. DALI-väylään liitetyistä LED-valaisimista työtehoa alentavaksi voi olla yksi kybervaikuttamisen tavoite. Kuvio 2 havainnollistaa valon aallonpituuden merkitystä näkemiselle ja vireystilalle. Heikko, hämärä valaistus vähentää vireyttä lisäämällä sitä säätelevän melatoniinin tuottoa, mutta kylmänä koettava, värilämpötilaltaan korkea ja lyhytaaltoinen sininen valo tukahduttaa melatoniinin tuotannon. Tällöin vireystila ei alene, vaikka näkemisen kannalta valoisuus ei juuri muuttuisikaan. Työpaikoilla valaistuksen sävy voi tarkoituksellisesti olla keskipäivällä sinisävyinen post-lunch-dip-efektin vähentämiseksi, joka kybervaikutuksella voidaan haluta kumota.



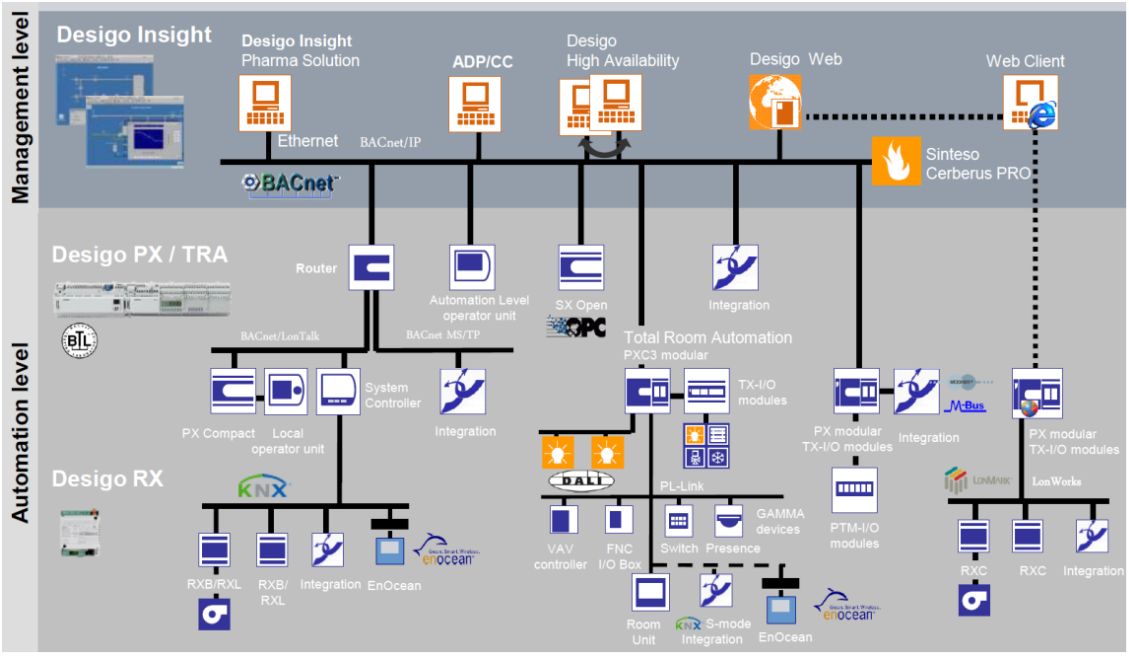
KUVIO 2. Valon aallonpituuden vaikutus vireystilaan (sininen) ja näköherkkyyteen (punainen). (van Bommel & den Beld 2003)

3.2 Alakeskukset sekä huone- ja yksikkösäätimet

> Alakeskukset ohjaavat kenttälaitteiden toimintaa sekä ottavat vastaan kentältä tulevat viestit. Säädettävät, ohjattavat ja valvottavat toiminnot on liitetty alakeskuksiin I/O-pisteiden välityksellä (AI, AO, DI, DO). Huonesäätimillä, joihin myös liittyy kohdekohtainen sovellusohjelmisto, hallitaan yhden huoneen tai huoneen osan olosuhteita (mm. jäähdytyspalkit, konvektorit, lämmityspatterit, valaistus) siihen liitettyjen kenttälaitteiden avulla. Huonesäätimiä on myös itsenäisinä säätiminä ilman väyläliityntää, jolloin kyseessä on yksikkösäädin. Alakeskusohjelmisto koostuu perusohjelmistosta ja sovellusohjelmistosta. Sovellusohjelmistossa sijaitsevat mm. kohdekohtaisten säätöjen, ohjauksien, indikointien ja hälytysten hallintaan liittyvät sovellukset kuten säätö-, aika- ja tapahtumaohjelmat. Huonesäätimien ohjelmat koostuvat joko kiinteistä vakio-ohjelmista tai perus- ja sovellusohjelmistosta. (ST 98.17 2018, 2 – 3.)

Edellisestä määrittelystä poiketen yksikkösäädin voi olla myös väyläliitännällä varustettu ja ne ovat ilmeisesti yleistymässä. Esimerkiksi melko yleinen iv-koneen yksikkösäädin Ouman EH-105 voidaan liittää sovittimella Modbus/RTU -väylään ja sitä kautta muihin laitteisiin kuten Schneider Electricin Modicon M17x säätimet voidaan liittää useilla protokollilla Ethernet verkkoon. (ST-käsikirja 17, 95)

Väylien ja protokollien osalta automaatiotaso, jota alakeskukset edustavat, on myös silta hallinto- ja kenttätasojen välillä. Koska myös automaatiotasolla voi esiintyä valmistajista tms. johtuen eri väylätyyppejä ja protokollia, niin alakeskus voi joutua käsittelemään vaikkapa kuutta eri väylätyyppiä ja kymmentä eri protokollaa osana laajempaa järjestelmäkokonaisuutta. Tämä luo vähintään lisää haasteita erilaisten turvallisuusaspektien hallintaan mm. järjestelmien ohjelmarevisioiden yhteensopivuuden varmistamisessa.
Kuvassa 6 on esimerkki ratkaisusta, jossa on käytetty useita eri väyliä ja protokollia.



KUVA 6. Esimerkki automaatiojärjestelmän kokoonpanosta (Siemens Building Technologies, n.d.)

Alakeskusten ja eri säätimien ohjelmat ovat ensisijaisesti niitä, joihin kohdistetulla kybervaikuttamisella pyritään saamaan haluttu tila tai toiminnallisuus aikaan. Vaikutuksen kohteena ei tarvitse olla itse säätöprosessi tms., vaan tavoite voidaan saavuttaa esim. ylikuormittamalla säätimen yhteiskäyttöinen prosessori turhalla tietoliikenteellä, jonka seurauksena säätimen aliohjelmalle ei riitä suoritusaikaa ja säätö jää tekemättä. Kohdistetumpi kybervaikuttaminen edellyttää jollakin tavalla aiheutettua muutosta automaatioohjelmiston toimintaan. Vaikutus voi olla ennalta suunnitellusti toimiva haittaohjelma, jonka käynnistää jokin tapahtuma, tilayhdistelmä tms. tai sitten se voi olla dynaaminen, ihmisen ohjauksen perusteella johonkin prosessiin kohdistuva muutos. Jälkimmäinen edellyttää reaaliaikaista yhteyttä automaatiojärjestelmän ao. osaan, mutta reitti siihen voi olla toteutettu minkä tahansa ulkoisen liitynnän tarjoavan osan kautta.

Talotekniikkasuunnittelijalla on hyvin vähän keinoja vaikuttaa ohjelmistoihin kohdistuviin uhkiin ja riskeihin. Ohjelmistoihin kohdistuva vaikuttaminen voidaan havainnoida ja osin jopa estää ulkoisin järjestelmin, esim. IDPS:llä (tunkeilijan havaitsemis- ja estojärjestelmä), mutta hyvällä ohjelmistosuunnittelulla ja toteutuksella on haittojen pienentämisessä merkittävä osuus. RASP (ohjelman suorituksen aikainen itsesuojelu) on yksi mahdollinen teknologia, jonka voi implementoida järjestelmään parantamaan kybervaikuttamisen uhalta suojautumista. Mutta talotekniikkasuunnittelijan vastalääkkeet ovat

niitä kenttälaitteiden yhteydessä esitettyjä ratkaisuja nopeaan ja hallittuun omavoimaiseen säätöön tms. siirtymiseksi silloin, kun erilaiset automaatiojärjestelmät ovat tai on laitettava toiminnasta pois.

3.2.1 DoS

Prosessointikyvyn estävästä tai sitä rajoittavasta vaikutustavasta ylikuormittamalla prosessori käytetään nimitystä DoS ja sillä tarkoitetaan palvelunestohyökkäystä. Jos hyökkäys tapahtuu hajautetusti monesta lähteestä, niin nimitys on DDoS. Alussa mainittu esimerkkitapaus Lappeenrannasta oli Enermix Oy toimitusjohtaja Janne Heinosen IoT-seminaarissa 18.4.2018 kertoman mukaan DoS -hyökkäys. Sen seurauksena kohteen lämpötilasäädölle ei enää riittänyt CPU aikaa, eikä menoveden lämpötila enää muuttunut olosuhteiden muutoksen mukaisesti.

DoS voidaan toteuttaa hyvin monella mekanismilla optimoiden mm. vaikutukseen tarvittava tietoliikenteen määrä kohdeprosessin ominaisuuksien mukaan. Suojautumismenetelmät perustuvat tietoliikenteen analysointiin ja suodattamiseen sellaisin toteutuksin, jotka eivät vaaranna itse pääprosessin toimintaa.

3.2.2 Logiikkapommi

Logiikkapommi on yksi vanhimmista kybervaikutuksen käynnistävistä mekanismeista. Järjestelmän ohjelmistoon ujutetaan halutun toiminnallisuuden aiheuttava koodi esimerkiksi tarkastamattoman ohjelmistopäivityksen tai jonkin USB:n käytön yhteydessä, jollei se ole ollut siellä jo alusta alkaen. Pommi odottaa suoritushetkeä, joka voi olla joku ulkolämpötilan ja kosteuden kombinaatio tai joku ajanhetki. Pommin koodi voi olla pieni sen havaittavuuden vaikeuttamiseksi, mutta käynnistyttyään se voi avata takaportteja laajemman vaikutuksen aiheuttavan koodin syöttämiseksi. Koska säätimet sisältävät usein valmistajakohtaisia erikoispiirejä, on niihin voitu kätkeä tarvittava koodisto jo valmistuksen yhteydessä valmistusmaan viranomaisten vaikutuksesta. Tällaiset tekniikat ovat tuskin tarkoitettu yksittäiseen käyttöön, vaan niiden avulla tähdätään laajempaan vaikutukseen. Jos esimerkiksi yleisten rakennusautomaatiomerkkien O, F ja S säätimien ohjaamat kaukolämmön säätöventtiilit saadaan -20°C lämpötilassa sulkeutumaan yhtäaikaisesti koko

verkoston alueella, niin vaikutukset eivät rajoittune vain jäähtyviin taloihin, kun voimalaitokselta poistuu iso kuorma nopeasti ja ennakoimatta.

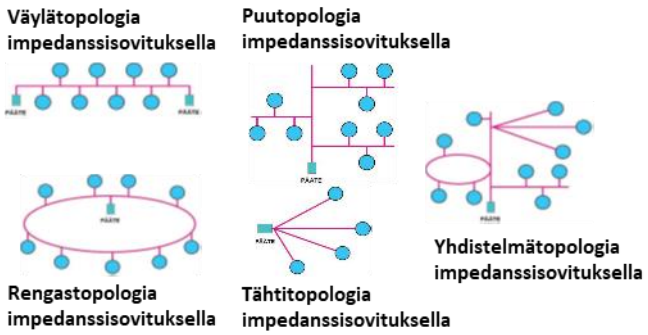
3.2.3 Väylät ja protokollat

Automaatiojärjestelmän tiedonsiirto voi olla toteutettu hyvin monella tavalla topologian, väylien ja protokollien osalta. Riippumatta toteutustavasta rakennusautomaatiojärjestelmän eri osien välillä siirretään tietoa kuhunkin tarkoitukseen soveltuvalla tavalla. Tiedonsiirron pitää täyttää kolme perusvaatimusta (luottamuksellisuus, eheys ja saatavuus, LES tai CIA), jotta sen varaan voidaan toteuttaa muita toimintoja.

Tieto on luottamuksellista, jos se voi olla siihen oikeudettoman hallussa luvallisille osapuolille haittaa tai vaaraa aiheuttava. Mitättömältä vaikuttavat yksittäiset tiedot voivat esim. muuttua pitkältä ajalta kerättynä kiusalliseksi kokonaisuuksiksi tai myyntiartikkeleiksi, ja lisäksi sanomissa voi olla myös käyttäjätunnuksia ja salasanoja, jotka helpottavat esim. identiteettivarkauksien tekemistä. Luottamuksellisuuden säilymistä edesauttaa tiedonsiirron salaaminen menettelyllä, johon liittyvä salausavaimen ja tiivisteen käyttö tuottavat myös tiedon eheyden varmistavan osuuden. Salaus vaikuttaa saatavuuteen yleensä heikentävästi, koska salatun ja kaikin puolin varmennetun yhteyden ja tiedonsiirron toteutus vaatii prosessointiaikaa sekä lisää tiedonsiirron fyysisen kerroksen kuormaa aiheuttaen ainakin jonkinlaista viivettä. Yleensä tämä ei ole mikään ongelma valvomoihin liityttäessä, ja koska vaikuttamispyrkimykset ovat ehkä parhaiten toteutettavissa ulkoisen yhteyden kautta, niin vähintään yhteys valvomoon tulee salata asianmukaisesti.

Väylä- ja protokollavalinnat on tehtävä huolella, jotta varsinainen toiminnallisuus voidaan taata, mutta silti huolehtia myös vaadittavasta tieto- ja kyberturvallisuudesta. Käytännössä tilanne on kielteisessä mielessä hieman yksinkertaisempi, koska missään puhtaasti automaatiojärjestelmille tarkoitetussa väylä- tai protokollaratkaisussa ei ole kunnollista salausta ja käyttäjien autentikointia sisäänrakennettuna. Kaikkine puutteineenkin TCP/IP tarjoaa kuljetus- ja verkkokerroksille käyttökelpoisen ratkaisun, johon tukeutuvia sovelluskerroksen sisällön turvalliseen siirtoon tarvittavia palveluita on tarjolla useita. Bithouse Oy:n tj Tommi Nummelinin mukaan uusimpien toteutusten web service -ratkaisut alkavat olemaan turvallisuuden kannalta useimpiin tapauksiin riittävät (Nummelin, 2018).

Topologiassa on hyvä erottaa fyysisen verkon topologia ja toimintojen kannalta looginen topologia. Edellisellä on vikasietoisuuteen suuri merkitys, mutta kyberturvallisuuteen vaikuttaa lähinnä valvottujen laitetilojen ulkopuolelle johdetut verkon osat ja niiden suojaus. Loogisella topologialla toiminnot segmentoidaan siten, että sisäisten palomuurien avulla voidaan rajoittaa tiedonsiirto vain haluttujen osien välille ja näin kiistää johonkin verkoston osaan tunkeutumaan päässeen mahdollisuuksia vaikuttaa laajemmin järjestelmään. Ratkaisulle on vielä enemmän tarvetta, kun automaatioon integroidaan muuten huonosti tunnettuja osia, kuten lukitusten hallinta ja palo- tai rikosilmoitusjärjestelmä. Kuvassa 7 esitetään yleisimmät fyysiset verkkotopologiat.



KUVA 7. Yleisimmät fyysiset verkkotopologiat (yhdistelmä ST-käsikirja 21 kuvista 4.1 – 4.6 pl. 4.5)

3.3 Valvomot

Valvomot ovat automaation hallintotasolla, eivätkä ne osallistu varsinaiseen säätöön tai ohjaukseen. Valvomo-ohjelmiston avulla voidaan asettaa esim. tavoitearvoja lämpötilalle, johon automaatiotason alakeskus tai yksikkösäädin alkavat säädön lopputuloksella pyrkiä. Mikäli automaatiotasolla ei ole asetettu mitään rajoitteita, niin lopputulos voi olla mitä vain laitetasolla mahdollisesti sallituksi asetetuissa rajoissa. Ylilämpöä tai sähkötehoa voi rajoittaa automatiikasta riippumatta helposti, mutta alilämmöltä ja jäätymiseltä suojautuminen on hankalampaa.

Valvomo-ohjelmistoon voidaan toteuttaa erilaisia hälytyksiä tarvittavien toimenpiteiden käynnistämiseksi. Hälytykset voivat tulla myös suoraan kenttälaitteilta tai automaatiotasolta, jolloin ne käsitellään luokitustaan vastaavalla tavalla. (ST-käsikirja 17, 224.) Yksi

kybervaikuttamisen tapa voi olla se, että aiheutetaan sen verran virheellisiä hälytyksiä, että käyttäjät kyllästyvät niihin ja hälytykset estetään virheellisinä kokonaan ja vasta tämän jälkeen aloitetaan itse asiaan vaikuttaminen. Toinen tapa voi olla esimerkiksi sellainen, jossa säätimen asetusarvoa muutetaan pienin askelin kohti tavoitetta, jotta mahdollinen muutosnopeutta valvova suoja ei toimisi. Yksinomaan pelkkiin valvomon tuottamiin tai välittämiin hälytyksiin ei kannata turvata missään tilanteessa, vaan prosesseja on tarkkailtava aktiivisesti poikkeamien havaitsemiseksi. (ST-käsikirja 17, 227.)

Valvomot ovat usein tavallisia tai hieman kovennettuja PC-laitteistoja, jotka voivat olla varustettu automaatiotasoon liittymiseksi tarvittavalla tiedonsiirtosovittimella. Mikäli valvomo on yhteinen monelle kiinteistölle tms., niin toiminnallisuus sisältää myös näyttöjen vuorotteluun ja valintaan liittyvät osat. Jos valvomon ja alakeskuksien välistä tiedonsiirtoa ei turvata jollakin riittävän turvallisella ohjelmallisella ratkaisulla, on siirtokerrokseen toteutettava erillisin laittein tarvittavat turvaominaisuudet. Ajoalustan virtualisointi on hyvä menettely pienentämään kybervaikuttamisen riskiä ja nopeuttamaan vakavista häiriötilanteista palautumista. Virtualisoinnilla tarkoitetaan yhden tai useamman varsinaista sovellusta ajavan käyttöjärjestelmän suoritusta yhdessä luotettavana pidettävässä tietokoneessa. Oikein tehtynä järjestely on melko hyvä rajoittamaan sekä tahallisten vaikutuspyrkimysten, että häiriötilanteiden leviämistä laajemmalle kuin ao. valvomon virtuaaliympäristöön. Virtualisoinnilla voidaan myös säästää kustannuksissa ja helpottaa ylläpitoon liittyviä rutiineja.

3.4 Muu taloautomaatio

Talotekniikan toimintaa ohjaavan automaation lisäksi rakennuksissa on usein muitakin järjestelmiä, jotka ovat joko tarpeen liittää tai ne vain halutaan liittää laajemmaksi taloautomaatioksi (taulukko 2). (ST-käsikirja 17, 150) Pumppaamot on mainittu jo aiemmin kenttälaitteiden kohdalla, mutta muista yleisimmät lienevät paloilmoitin- sekä savunpoisto- ja palopeltijärjestelmät, joilla on toiminnallinen yhteys ilmanvaihtoon ja turvavalaistukseen. Muita voivat olla esim. lukitus-, kulunvalvonta- ja rikosilmoitusjärjestelmät, joista löytyy toiminnallinen yhteys mm. sisä- ja ulkovalaistuksen ohjaukseen sekä em. paloilmoitusjärjestelmään. Varavoimajärjestelmät, jonka yksi osa katkoton jännitesyöttö (UPS) on, ovat harvoin asuinrakennuksissa esiintyviä, mutta suurissa kiinteistöissä ja

esim. paljon tietotekniikkaa tai jäähdytystä käyttävissä kohteissa aivan yleisiä. Varavoiman ja UPS:ien käyttö osana kysyntäjouston elementtejä on hyvä peruste liittää ne kohteen rakennusautomaatioon. VTT:n DyRES-projektissa tehdyssä simulaatiossa Jyväskylän Hippoksen alueen uudistukseen (kuva 8) liittyen pelkästään sähkön kysyntäjouston osalta voidaan saavuttaa n. 15% säästö energiakustannuksissa.

KUVA 8. Jyväskylän Hippoksen alueen tulevaisuuden visio (VTT 2017)

Vaikka kukin kokonaisuuteen liitetty erillisjärjestelmäkin on omana kohteenaan altis kybervaikutuksille, niin ne voivat myös muodostaa väylän kohdistaa kybervaikutus johonkin toiseen kokonaisuuden osaan. Ei siis riitä, että asettaa vaatimukset vain jollekin kokonaisuuden osajärjestelmälle, vaan samat turvallisuusvaatimukset on asetettava kaikille järjestelmille ja niiden ylläpito-organisaatiolle. Tämä on huomioitava tarvittaessa tilojen järjestelyissä, lukituksissa jne. sekä etenkin suunniteltaessa ja toteutettaessa kokoonpanojen muutoksia sekä ohjelmistopäivityksiä. Muuten esimerkkinä mainitun Hippoksen

alueen kaltaisissa kohteissa laskennalliset energian säästöt saattavatkin muuttua lisäkustannuksiksi, kun kysyntäjousto ei toimi tarkoitetulla tavalla esim. kybervaikuttamisen johdosta.

TAULUKKO 2. Erillisjärjestelmiä kiinteistötyypeittäin (Eklund 2008)

	Liike-kiinteistöt	Terveydenhoito-kiinteistöt	Oppilaitokset	Asuinrakennukset	Teollisuusrakennukset	Toimistorakennukset	Julkiset rakennukset
Rikosilmoitusjärjestelmät	X	X	X		X	X	X
Kulunvalvontajärjestelmä	X	X	X		X	X	X
Paloilmoitinjärjestelmät	X	X	X		X	X	X
Sisä- ja ulkovalaistusjärjestelmät	X	X	X	X		X	X
Turvavalaistusjärjestelmät	X	X	X		X	X	X
Pumppaamot	X	X	X	X	X	X	X
Äänentoisto- ja kuulutusjärjestelmät	X	X	X				X
Savunpoisto- ja palopeltijärjestelmät	X	X	X		X	X	X
Hissit, liukuportaat, kuljettimet	X	X	X	X	X	X	X
Lääkintätilojen sähköjärjestelmät		X					
Kaasuvalvontajärjestelmät		X			X		
Varavoimajärjestelmät		X			X		
Muuntajat ja kompensointijärjestelmät	X	X	X		X	X	X

4 SUOJAUS JA YKSITYISYYS SEKÄ SOPIMUKSET

4.1 Fyysinen suojaus ja käyttöoikeuksien hallinta

Talotekniikan kyberriskin hallinnassa myös fyysisellä suojauksella on oma merkityksensä. Laite- ja valvomotiloihin pääsyn tulee olla valvottua ja käyntejä tulee myös valvoa. Laitetilojen ulkopuolelle johdetut väylät mahdollistavat vapaan pääsyn järjestelmään, mikäli riittäviä turvaamistoimia, kuten esim. em. segmentointeja, ei ole tehty.

Automaatiojärjestelmään pääsyn omaavan henkilöstön ja siihen kytkeytyvien eri palveluiden käyttöoikeuksien hallinta on yksi keino pyrittäessä turvaamaan talotekniikkaa kybervaikuttamiselta. Kaiken ei tarvitse olla mahdollista kaikille eikä lopuillekaan aina, ja silti hyvä käytettävyys voidaan saavuttaa harkitulla oikeuksien hallinnalla. Roolit ovat yksi tapa hallita oikeuksia ja se voidaan toteuttaa myös joustavasti. (ST-ohjeisto 22, 18; ST-käsikirja 17, 160)

Kun suojataan ja rajoitetaan, niin toimiin täytyy liittyä myös valvonta esim. lokien muodossa. Vaikka. kohteessa käy luvallinen henkilö, niin käyntiin pitää olla joku syy. Lokien perusteella tehtävän tapahtumatarkastelun tulee nostaa esille normaalista poikkeavat tapahtumat, jotta mahdolliset virheet tms. voidaan korjata ajoissa. Jos jotain ikävää ilmenee, niin asialliset lokitiedot auttavat selvittämään tapahtumat ja helpottavat tarvittavien korjausten tekemistä vastaisuuden varalle. (ST-ohjeisto 22, 19)

Ainakin sellaisiin käynteihin, joissa on tarkoitus muuttaa jotakin asetusta tai muuttaa järjestelmäkonfiguraatiota, pitää olla kaksivaiheinen kontrolli. Tällöin esim. tekninen isännöitsijä valtuuttaa toimen ja myös valvoo sen tapahtumisen. Sama koskee etänä tehtäviä aktiviteettejä, kuten mm. ohjelmistopäivitykset. Kaikki muutosten tekemisen mahdollistavat palvelut ja toiminnot sekä ulkoiset muistivälineet voivat olla oletusarvoisesti kytketty pois käytöstä pl. teknisen isännöitsijän rooli, jolla on oikeus aktivoida tarvittavat oikeuden muutokset muille rooleille, joko fyysisille tai virtuaalisille.

Suojaus ja kontrolli tulee luonnollisesti suhteuttaa riskiin ja etenkin sen vaikuttavuuteen. Yhden perheen omakotitaloon vaikuttaminen on harmillista, mutta viiden perheen rivita-

lossa vaikutukset ovat samalla vaivalla moninkertaiset. Jos kohteena on isompi, 50 asunnon kerrostalo, niin vaikutukset kertaantuvat ja laajentuvat väistämättä myös moneen työyhteisöön, vaikka suoranainen vaikutus olikin kohdistettu vain asuntoihin.

4.2 Yksityisyyden suojaus

Vaikka automaation keräämästä datasta voidaan tehdä paljon hyviä ja hyödyttäviä analyysejä taloteknisten järjestelmien optimoimiseksi, niin varjopuolena on tietovarannon vääriin käsiin joutumisen mahdollisuus. Jos tietoja tallennetaan ilman anonyymisointia, niin teknisten tietojen lisäksi voi karata myös henkilötietoja, joiden suojausvaatimukset (GDPR) määrittävät tietojen keräämiselle ja käytölle tiukat kriteerit. Järjestelmän teknisestä toiminnasta kerätyn tiedon perusteella voidaan esim. luoda malli, jonka avulla kybervaikuttamista voi kohdentaa. Yhdistämällä mm. kulutustietoja henkilötietoihin, jollainen esim. huoneiston numero on, voidaan luoda henkilöprofiili, jota vuorostaan voi pyrkiä hyödyntämään monin tavoin. Yksityisyyden suoja on otettava jatkossa vakavasti huomioon kerättäessä ja luovutettaessa talotekniikasta saatavissa olevaa mittaustietoa. Tiukempi säännöstö ei ole este tarvittaville toimille esim. automaation optimoimiseksi, mutta laillisuuden varmistamiseksi asiat on vain tehtävä hieman toisin, kuin aiemmin on ollut tapana.

4.3 Sopiminen

Talotekniikan ylläpidossa on omat sopimuskäytäntönsä ja yleiset sopimusehtonsa. Kiinteistöpalvelualan yleiset sopimusehdot 2007 (KP YSE 2007) määrittää yleispiirteisesti osapuolten velvoitteet ja vastuut, joten yksityiskohtaisempi sopiminen on vähintään suositeltavaa. (ST-ohjeisto 22, 14) Esimerkiksi tietosuojan osalta 21 §:ssä määreenä on lainsäädännön noudattaminen, mutta tiedostavatko sopijapuolet mitä tuo tarkoittaa esim. EU-tasoisista määräyksistä alkaen johdettuna? Samaa voi miettiä 6 § kohdalla avainten hallintaan liittyen, johon myös pääsyoikeudet eri järjestelmiin tulee rinnastaa.

Isännöintipalvelujen yleiset sopimusehdot ISE 2007 on laadittu lähes saman tasoisesti kuin KP YSE 2007 ja tietoturvaan liittyvät asiat määritellään 16 §:ssä. Lisäksi sopimuksen käsitteet määrittävässä osassa on tietosuoja ja tietoturva määritelty asianmukaisesti.

Vaikka kiinteistöjä hoitaville henkilöille on mahdollistettava tarvittava pääsy mm. automaatiojärjestelmiin, niin pääsyoikeuksien rajaamista tarpeen mukaiseksi ei ainakaan yleisissä sopimusehdoissa vaadita em. avainvertausta enempää. Tilaajana asunto-osakeyhtiön on syytä tarkastella huolella kaikki sopimusehdot ja vakavasti harkita kunnossapitohenkilöstölle asetettavia vaatimuksia ja kontrolleja. On hyvä huomioida se, että talotekniikan tieto- ja kyberturvallisuuden parantuessa helpoimmaksi keinoksi päästä järjestelmiin käsiksi muodostuu aina vain useammin talotekniikan parissa työskentelevä ihminen, jonka tahaton virhe tai tahallinen toiminta avaa tarvittavan kanavan. Tahallisen toiminnan riskiä voi pyrkiä pienentämään turvallisuusselvityslain 726/2014 22 § mahdollistaman turvallisuusselvitysmenettelyn käytöllä, johon SUPO voi harkintansa perusteella hakemuksesta suostua. Kiinteistöhuoltohenkilöstön työmotivaatiota voi myös pyrkiä parantamaan yhtenä keinona inhimillisten riskien hallitsemiseksi. Koulutus ja palkkaus voivat parantaa sitoutumista ja pienentää houkutusta tai tarvetta harmia aiheuttavalle toiminnalle. (ST-käsikirja 17, 266)

5 POHDINTA

Talotekniikan kyberturvallisuuteen on alettu kiinnittämään selvästi enemmän huomioita jo sillä perusteella, että muutamana viime vuotena on julkaistu asiaan liittyvää ohjeistusta mm. ST-kortistossa. Tavallista talotekniikkasuunnittelijaa, isännöitsijää tai asunto-osakeyhtiön hallituksen jäsentä ohjeistus ei kuitenkaan liene vielä tavoittanut. Tilannetta voisi parantaa sillä, että ST-korteissa julkaistuja hyviä ohjeita julkaistaisiin myös RT- ja KH-korteissa, jolloin ne leviäisivät sähköalan toimijoita laajemman piirin tietoisuuteen. Myös kuntoarvioiden laatimiseen liittyvissä ohjeissa ja malleissa rakennusautomaation selvempi huomioiminen auttaisi eri osapuolia kiinnittämään huomiota talotekniikan kyberriskeihin ja niiden hallintaan. Asunto-osakeyhtiöissä on nimetty usein hallituksen tueksi joku väestönsuojeluun paremmin orientoituva henkilö tai tiimi, johon tehtäväkuvaan voi hyvin lisätä myös muiden, ehkä todennäköisempien, riskien hallintaan liittyvät tehtävät, kuten esimerkiksi kyberriskit tai rakennusautomaation vakavasta häiriötilanteesta toipumisen suunnitelmat. Tällöin sekä ylläpitoa toimeenpanevat, että yhtiön puolesta asioita hoitava tekninen isännöitsijä tulisivat tietoisemmiksi varautumisen tasosta, joka omalta osaltaan auttaa pahimman häiriötilanteen hallinnassa ja siitä toipumisessa.

Talotekniikan suunnittelija voi ottaa kyberriskit huomioon suunnittelemalla automaation rinnalle sähköisestä rakennusautomaatiosta riippumattoman, tarpeen mukaan käyttöön otettavan säätöjärjestelmän kiinteistön käytön kannalta kriittisimmille toiminnoille, kuten lämmitykselle, lämpimälle vedelle ja ilmanvaihdolle, mahdollisesti jopa jäähdytykselle. Lisäkustannus tilaajalle ei ole kovin suuri, mutta varautuminen mahdollistaa käytön jatkamisen automaation pettäessä syystä tai toisesta.

Erilaiset älykodit, -talot, -korttelit ja -kaupungit tähtäävät asumisen laadun paranemiseen sekä energiakustannusten pienentämiseen monin tavoin. Ikävä kyllä kaikki ne lisäävät kybervaikutuksen riskiä niin todennäköisyytenä kuin vaikuttavuutena. Riskien pitämiseksi siedettävällä tasolla on niiden hallintaan panostettava laatimalla suunnitelmat huolella ja valvomalla toteutusta ja käyttöä entistä paremmin. Tekniikan koventuessa on heikoimmaksi lenkiksi muodostumassa entistä selvemmin ihminen, joka voi omasta virheestään, halustaan tai pakotettuna aiheuttaa paljon harmia ja haittaa niin talotekniikan toiminnalle kuin siihen liittyvälle yksityisyyden suojaan kuuluvilla tiedoilla.

LÄHTEET

Asetus 2016/679/EU. Euroopan parlamentin ja neuvoston asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus). Euroopan unionin virallinen lehti 4.5.2016. Luettu 15.5.2018. http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016R0679

Direktiivi 2016/1148/EU. Euroopan parlamentin ja neuvoston direktiivi toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa. Euroopan unionin virallinen lehti 19.7.2016. Luettu 15.5.2018. http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016L1148&rid=1

Eklund, K. 2008. Erillisjärjestelmien liittäminen rakennusautomaatiojärjestelmään. Tampereen ammattikorkeakoulu. Sähkötekniikan koulutusohjelma. Opinnäytetyö.

Hakala, P. & Kaappola, E. 2013. Kylmälaitoksen suunnittelu. 3.painos. Helsinki: Opetushallitus.

Huovinen, A. 2017. Joustavaa energiankulutusta on hyödynnettävä tehokkaammin osana energiajärjestelmää − kuluttajan tarpeet huomioiden. VTT:n Blogi 20.6.2017. Luettu 15.5.2018. https://vttblog.com/tag/kysyntajousto/

KATAKRI. 2015. Tietoturvallisuuden auditointityökalu viranomaisille. Helsinki: NSA/Ulkoministeriö.

KH-kortti X4-00404. 2008. Isännöintipalvelujen yleiset sopimusehdot ISE 2007. Helsinki: Rakennustieto.

KH-kortti X4-00405. 2008. Kiinteistöpalvelualan yleiset sopimusehdot KP YSE 2007. Helsinki: Rakennustieto.

KYBER-TEO 2014. 2017. KYBER-TEO – tuloksia 2014–2016. Julkisten tulosten kooste. VTT 298. Espoo: VTT.

Laajalahti, M. & Nikander, J. 2017. Alkutuotannon kyberuhat. Luonnonvara- ja biotalouden tutkimus 32/2017. Helsinki: Luonnonvarakeskus (LUKE)

Luukkanen, J. 2005. Suomen pitkän aikavälin kehitys: arvioita ja visioita. Verkkovisio 2030 –hankkeen työpaja. (Kumpulainen, L. n.d. Toimintaympäristön muutos. Vaasan yliopiston diasarja, 33. Luettu 15.5.2018. http://vaasanseutu.fi/app/uploads/sites/7/2015/06/Kumpulainen-Lauri-Vaasan-yliopisto.pdf)

LVI-ohjekortti LVI 01-10259 / KH 90-00226. 1996. Tarkastus-, hoito- ja huolto-ohjeet. Poikkeus- ja häiriötilanteiden ohjeet. Asuintalon huoltokirja. Rakennustieto Oy.
Nummelin, T. toimitusjohtaja. 2018. Haastattelu 11.5.2018. Haastattelija Järvinen, A. Jyväskylä

Ollenberg, J. 2015. Verkottuneen talotekniikan tietoturva. Rakennustekniikan koulutusohjelma, YAMK. Metropolia Ammattikorkeakoulu. Opinnäytetyö.

Pietiläinen, Kauppinen, Kovanen, Nykänen, Nyman, Paiho, Peltonen, Pihala, Kalema & Keränen. 2007. ToVa-käsikirja. VTT 2413. Espoo:VTT.

Pullinen, M-J. 2012. Kriittisten tietojärjestelmien suojaaminen kyberuhilta. Laurea-ammattikorkeakoulu. Tietojenkäsittelyn koulutusohjelma, YAMK. Opinnäytetyö.

Rousku, K. Turvasatama. 31.10.2017. Ohjelmistojen päivitys ei enää riitä, uusi uhka on jo täällä. Luettu 10.12.2017. https://www.tivi.fi/blogit/ohjelmistojen-paivitys-ei-enaa-riita-uusi-uhka-on-jo-taalla-6684890

Siemens Building Technologies. n.d. Esimerkki automaatiojärjestelmän kokoonpanosta. Luettu 15.5.2018. https://conseils.xpair.com/consulter_savoir_faire/gestion_technique_batiment/architecture_gtb.htm#part-937

ST-kortti 710.02. 2017. Rakennusautomaation tietoturva. Espoo: Sähkötieto ry.

ST-kortti 730.05. 2017. Rakennusautomaatiojärjestelmän tietoturvan tarkastuspöytäkirja. Espoo: Sähkötieto ry.

ST-kortti 98.17. 2018. Rakennusautomaatiojärjestelmän kuntotutkimusohje. Espoo: Sähkötieto ry.

ST-kortti 98.44. n.d. Rakennusautomaatiojärjestelmän kuntotutkimuspöytäkirja. Espoo: Sähkötieto ry.

ST-käsikirja 17. 2012. Rakennusautomaatiojärjestelmät. Espoo: Sähkötieto ry.

ST-käsikirja 21. 2017. Kiinteistöjen tiedonsiirtoväylät. Tietotekniset järjestelmät. Espoo: Sähkötieto ry.

ST-käsikirja 22. 2017. Kiinteistöjen valvomojärjestelmät. Tietotekniset järjestelmät. Espoo: Sähkötieto ry.

ST-ohjeisto 22. 2015. Verkottuneen talotekniikan tietoturva. Espoo: Sähkötieto ry.
Suomen kyberturvallisuusstrategia 2013. Valtioneuvoston periaatepäätös 24.1.2013. Helsinki.

Tenkanen, T. 2016. Kiinteistöautomaatiojärjestelmän tietoturvakatsaus. Jyväskylän yliopisto. Tietotekniikan laitos. Pro gradu -tutkielma.

VAHTI. n.d. VAHTI-toiminta. Luettu 15.5.2018. http://vm.fi/vahti

van Bommel, W.J.M & den Beld, G.J. 2003. Lighting for work: visual and biological effects. Philips. (Brainard, G.C. 2002. “Photoreception for regulation of melatonin and the circadian system in humans”, Fifth International LRO lighting research symposium, Orlando.)